End to End Inter-domain Quality of Service Provisioning

Brewka, Lukasz Jerzy

Publication date:
2011

Document Version
Publisher's PDF, also known as Version of record

End to End Inter-domain Quality of Service Provisioning

Lukasz Brewka

December 2011

Networks Technologies and Service Platforms
DTU Fotonik
Technical University of Denmark
2800 Kgs. Lyngby
DENMARK

Preface

This thesis presents a selection of the research carried out during my Ph.D. studies in the Networks Technology and Service Platforms group, at Department of Photonics Engineer, Technical University of Denmark, from September 2008 to December 2011, under the supervision of Professor Lars Dittmann and Dr Henrik Wessing.

This Ph.D. study was mainly evolving around and received funding from project ALPHA "Architectures for fLexible Photonic Home and Access networks", which was part of the European Community's Seventh Framework Programme (FP7) under signature 212 352.

More than 6 months of the project period was a part of external stay in NetLab Department, Acreo AB, Sweden. Results presented in Chapter 5 were obtained in networking laboratories of Acreo AB - NetLab.

The external research stay at Acreo AB was funded by project ALPHA. Expenses connected to travels for international conferences were co-financed by Otto Mønsted Fond.

Abstract

This thesis addresses selected topics of Quality of Service (QoS) provisioning in heterogeneous data networks that construct the communication environment of today's Internet. In the vast range of protocols available in different domains of network infrastructures, a few chosen ones are discussed and their key QoS features are analysed.

This thesis mainly focuses on home and access networks, and their interaction. Considering home networks, UPnP-QoS Architecture was chosen in order to analyse the possibilities of QoS provisioning at users' premises using service oriented architectures. First, the general UPnP-QoS performance was assessed analytically and confirmed by simulations results. The results validate the usability of UPnP-QoS, but some open issues in the specification were identified. As a result of addressing mentioned shortcomings of UPnP-QoS, a few pre-emption algorithms for home gateway were designed and compared. Similarly as for general UPnP-QoS assessment, analysis and intensive simulations were used for verification of proposed pre-emption techniques. The other proposed extension for UPnP-QoS was an integration of traffic auto-classification within UPnP-QoS Architecture. Simulation results of this extension showed the potential of this method in QoS preservation for scenarios where UPnP non-compliant devices are present in home networks.

With well defined ideas about home QoS, the interdomain aspects of QoS provisioning were addressed. For access network control the Generalized Multi-Protocol Label Switching (GMPLS) protocol suite was selected. Its growing popularity in access networks together with its maturity and wide adoption in core networks, makes it a great candidate as an end-to-end QoS provisioning mechanism. As a consequence of the UPnP-QoS/GMPLS mapping analysis and design, an OSGi-based inter-

face was developed. It allows integrated QoS establishment, initiated by UPnP-QoS Control Point and configuring home devices, then passing the Home Gateway, and finally triggering Label Switching Path establishment in the access network. To depict the versatility of the GMPLS suite and discuss also access Passive Optical Network (PON) technologies, a GMPLS controlled Ten Gigabit Passive Optical Network (XG-PON) was proposed. This part of the thesis introduces the possibility of managing the XG-PON by the GMPLS suite, showing again that this protocol suite is a good candidate for an integrated QoS solution. Additionally, one can notice that such a GMPLS controlled XG-PON could be connected with UPnP-QoS/GMPLS interface and GMPLS core, which is presented in this thesis, and which enables the end-to-end QoS also over PON links.

The final part of the thesis treats generalised concepts of resource reservation that could be used in core networks. Teletraffic engineering theorems are used for management of resources reserved for traffic of different priorities and rates in nodes, open and closed networks.

As a whole, this thesis can be seen as a QoS analysis starting from home networks through Home Gateways towards access links and finally reaching core networks - in this way constituting a path with end-to-end interdomain provisioned QoS.

Resumé

Denne afhandling omhandler udvalgte emner indenfor Quality of Service (QoS) provisionering i de heterogene netværk, som udgør det moderne Internet. Ud af den brede vifte af protokoller, som benyttes i de forskellige netværksdomæner, vil nogle få udvalgte blive diskuteret og analyseret med fokus på deres QoS funktioner.

Denne afhandling fokuserer primært på hjemme- og access-netværk og deres fælles interaktion. Med hensyn til hjemme-netværk, er UPnP-QoS arkitekturen blevet valgt for at analysere mulighederne for QoS provisionering på brugerens adresse ved hjælp af service orienterede arkitekturer. UPnP-QoS er først blevet undersøgt med hensyn til den generelle ydelse af protokollen gennem numeriske analyser, som herefter er blevet eftervist ved hjælp af computersimulationer. Resultaterne beviser brugbarheden af UPnP-QoS, men afslører også nogle åbne problemstillinger i specifikationen. I forbindelse med arbejdet med at løse disse begrænsninger er flere preemption algoritmer til hjemmerutere blevet udviklet og sammenlignet. På samme måde som for den generelle UPnP-QoS vurdering er disse algoritmer blevet verificeret både analytisk og gennem intensiv simulering. En anden udvidelse til UPnP-QoS er integreringen af autoklassificering af trafik indenfor UPnP-arkitekturen. Simuleringsresultater for denne udvidelse viser denne metodes potentiale med hensyn til QoS bevarelse i scenarier hvor hjemmenetværket også indeholder enheder, som ikke understøtter UPnP.

Med QoS på hjemmenetværket analyseret, er næste skridt at behandle interdomæneaspekterne af QoS provisionering. Til styringen af access-netværket er valget faldet på Generalized Multi-Protocol Label Switching (GMPLS) protokol suiten. Dens stigende popularitet i access-netværk sammen med dens modenhed og store udbredelse i core-netværk

gør denne suite til en oplagt kandidat til end-to-end QoS provisioneringsmekanismen. På baggrund af designet og analysen af sammenkoblingen mellem UPnP-QoS og GMPLS, er et OSGi-baseret interface blevet udviklet. Dette muliggør integreret etablering af QoS, initialiseret af et UPnP-QoS kontrol punkt gennem konfigureringen af enheder på hjemmenetværket, hvorefter signalet går ud gennem hjemmeruteren og endeligt initialiserer en Label Switch Path i accessnetværket. For at illustrere GMPLS suitens alsidighed, samt at diskutere access-netværk baseret på Passive Optical Network (PON) teknologier, foreslås et GMPLS-styret 10 Gigabit PON (XG-PON). Denne del af afhandlingen beskriver muligheden for at administrere et XG-PON gennem GMPLS suiten, hvilket igen illustrerer at protokol suiten er en god kandidat til en integreret QoS-løsning. Det er ydermere værd at lægge mærke til at et sådant GMPLS-kontroleret XG-PON vil kunne forbindes med det UPnP-QoS/GMPLS interface, som beskrives tidligere i afhandlingen, samt med GMPLS core-netværket, hvilket giver mulighed for end-to-end QoS, også over PON-forbindelser.

Den sidste del af afhandlingen behandler generaliserede koncepter i forbindelse med ressourcereservering i core-netværk. Her benyttes teoremer inden teletrafikplanlægning til at administrere ressourcereserveringen for trafik med forskellige prioriteter og hastigheder i knudepunkter, i åbne og i lukkede netværk.

Som helhed kan denne afhandling ses som en QoS-analyse, som går fra hjemme-netværk, gennem hjemmeruteren via access-forbindelsen og ender i core-netværket - og på denne måde skaber en forbindelse med interdomæne provisioneret QoS.

Acknowledgements

With their continued guidance, support and inspiration, I would like to thank my supervisors Professor Lars Dittmann and Dr. Henrik Wessing.

Thanks to Dr. Villy Bæk Iversen for numerous advices and great support, inspirations and ideas. Thanks to all the other colleagues in the Network Technology and Service Platform group: Dr. Lars Staalhagen, Dr. José Soler, Dr. Sarah Ruepp, Dr. Anna Vaseliva Manolova, Dr. Yin Yang, Dr. Hao Yu, Dr. Rong Fu, Dr. Jiang Zhang, Georgios Kardaras, Ana Rosselló-Busquet, Anders Rasmussen, Anna Zakrzewska, Jiayuan Wang, Thang Tien Pham, and Brian Sørensen.

I would like to thank the entire NetLab team in Acreo AB, special thanks to Pontus Sköldström, Anders Gavler and Victor Nordell for making me part of their group and help in the laboratory.

I would also like to thank all the people involved in ICT ALPHA project for a pleasant partnership and in particular Jelle Nelis, Dieter Verslype, Dr. Chris Develder for fruitful collaborations, and Dr. Michail Popov for a great coordination of the entire project.

Kgs. Lyngby, December 2011 Łukasz Brewka

Ph.D. Publications

This Ph.D. project has resulted in 20 peer-reviewed journal and conference publications and one publication in preparation.

The publications are listed below:

Published:

1. L. Brewka, H. Wessing, and L. Dittmann, "Signaling performance of UPnP QoS Architecture," in *Advanced Networks and Telecommunication Systems (ANTS), 2009 IEEE 3rd International Symposium on*, pp. 1 –3, December 2009.

2. R. Fu, M. Berger, Y. Zheng, L. Brewka, and H. Wessing, "Next Generation Network based Carrier Ethernet test bed for IPTV traffic," in *EUROCON 2009, EUROCON '09. IEEE*, pp. 1781 –1787, May 2009.

3. H. Wessing, M. S. Berger, H. Yu, A. Rasmussen, L. Brewka, and S. Ruepp, "Evaluation of Network Failure induced IPTV degradation in Metro Networks," ser. Electrical and Computer Engineering Series. World Scientific and Engineering Acad and Soc, pp. 135-139, 2009.

4. G. Kardaras, J. Soler, L. Brewka, and L. Dittmann, "Fiber to the antenna: A step towards multimode radio architectures for 4G mobile broadband communications," in *Fourth IEEE International Conference on Advanced Networks and Telecommunication Systems (ANTS) (IEEE ANTS 2010)*, (Mumbai, India), 12 2010.

5. L. Brewka, H. Wessing, and L. Dittmann, "Evaluation of lightweight preemption algorithms for UPnP QoS Architecture," in *Communications and Networking in China (CHINACOM), 2010 5th International ICST Conference on*, pp. 1 –5, August 2010.

6. J. Nelis, D. Verslype, C. Develder, L. Brewka, H. Wessing, and L. Dittmann, "Bandwidth reservations in home networks: Performance assessment of UPnP-QoS V3," in *Local Computer Networks (LCN), 2010 IEEE 35th Conference on*, pp. 272 –275, October 2010.

7. M. Popov, A. Gavler, P. Sköldström, and L. J. Brewka, "Integration of QoS provisioning in home and access networks: [invited]," in *Access Networks and In-house Communications , The Optical Society of America*, p. AWB6, June 2010.

8. L. Brewka, H. Wessing, and L. Dittmann, "UPnP QoS and queuing in home networks," in *Quality of Service (IWQoS), 2010 18th International Workshop on*, pp. 1 –2, June 2010.

9. H. Wessing, M. S. Berger, H. M. Gestssson, H. Yu, A. Rasmussen, L. Brewka, and S. Ruepp, "Evaluation of restoration mechanisms for future services using Carrier Ethernet," *WSEAS Transactions on Communications*, vol. 9, pp. 322–331, 2010.

10. L. Brewka, H. Wessing, A. Rosselló-Busquet, G. Kardaras, and L. Dittmann, "Network Based Control Point for UPnP QoS Architecture," in *The 8th Annual IEEE Consumer Communications and Networking Conference - Multimedia & Entertainment Networking and Services (CCNC'2011 - Multimedia & Entertainment Networking and Services)*, (Las Vegas, NV, USA), pp. 426–430, 1 2011.

11. L. Brewka, P. Sköldström, A. Gavler, V. Nordell, H. Wessing, and L. Dittmann, "QoS enabled resource allocation over an UPnP-QoS - GMPLS controlled edge," in *Consumer Communications and Networking Conference (CCNC), 2011 IEEE*, (Las Vegas, NV, USA), pp. 218 –222, Jan. 2011.

12. L. Brewka, H. Wessing, and L. Dittmann, "UPnP QoS Architecture and lightweight preemption algorithms," in *Consumer Communications and Networking Conference (CCNC), 2011 IEEE*, (Las Vegas, NV, USA), pp. 234 –236, Jan. 2011.

13. A. Rosselló-Busquet, L. J. Brewka, J. Soler, and L. Dittmann, "OWL Ontologies and SWRL Rules Applied to Energy Management," in *Computer Modelling and Simulation (UKSim), 2011 UkSim 13th International Conference on*, pp. 446 –450, 30 2011-april 1 2011.

14. J. Soler, A. Rosselló-Busquet, L. Brewka, M. S. Berger, and L. Dittmann, "Networks and services: A decade's perspective.," *Advances in Next Generation Services and Service Architectures*, 10 2010.

15. L. Brewka, P. Sköldström, A. Gavler, V. Nordell, H. Wessing, and L. Dittmann, "ALPHA: Proposal of mapping QoS parameters between UPnP home network and GMPLS access," in *SELFMAGICNETS Workshop, part of International ICST Conference on Access Networks (AccessNets) - 5*, (Budapest, Hungary), 2010.

16. J. Wang, L. J. Brewka, S. R. Ruepp, and L. Dittmann, "Cross Layer QoS Provisioning in Home Networks," in *Proceedings of OPNETWORK 2011*, (Wasington, USA), 2011.

17. L. Brewka, A. Gavler, H. Wessing, and L. Dittmann, "Proposal of QoS enabled GMPLS controlled XG-PON," in *2nd Internationale Workshop on Fiber Optics in Access Network - QoS and New applications (FOAN 2011)*, (Budapest, Hungary), Oct. 2011.

18. L. Brewka, P. Sköldström, J. Nelis, C. Develder, and H. Wessing, "Automatic Provisioning of End-to-End QoS into the Home," *Consumer Electronics, IEEE Transactions on*, vol. 57, pp. 1670-1678, November 2011.

19. L. Brewka, A. Gavler, H. Wessing, and L. Dittmann, "Including XG-PON under end-to-end GMPLS provisioned QoS", *Journal of Fiber and Integrated Optics*, vol. 31, no. 2, pp. 133-146, 2012.

Under review or in preparation:

20. L. Brewka, V.B. Iversen, and G. Kardaras, "End-to-end resource reservation for service-integrated networks".

Contents

List of Figures

List of Tables

Chapter 1

Introduction

The fact that we rely today on communication services in an increasing number of life aspects is undeniable. At the same time there is a tendency to put more and more of these communication services into a single data network, making the connection to our Internet Service Providers (ISPs) a communication and information highway between our homes and the rest of the world. HDTV streaming, VoIP calls, web browsing, cloud computing, all mentioned here services can be used over a single data link. The number of services offered in today's homes constantly grows. As these services often are essentially different from each other, they require different traffic handling in order to function properly. While in the past it was common to have a separate infrastructure for each service, today communication networks become more converged. That imposes problems of different services interfering with each other. Over-provisioning is a commonly used solution for addressing problems with service quality. Opinions about using over-provisioning vs. Quality of Service (QoS) are divided. Some claim over-provisioning is more economically justified than QoS provisioning [1], others notice that for certain applications over-provisioning cannot meet all the requirement [2,3]. Additionally, the cost of over-provisioning has increased with the migration to higher data rates [4]. Then, probably the closest to the truth is the statement that for some problems QoS is a more suitable solution and for others over-provisioning is better [5]. Summarizing, there definitely exists a need for QoS mechanisms in modern communication networks. Interrupted phone calls and video errors are not something that cus-

tomers bear easily, and one has to remember that over-provisioning gives no guarantees for traffic delivery. Another important fact is that QoS allows a smarter utilisation of resources. According to Internet Traffic Report on the average 15% of packets are lost - that is 1.6 TB of data lost every second in the World (as for 2011 [6]). Implementation of proper QoS mechanisms can improve these statistics, or at least lower their impact on selected traffic types.

The methods for QoS provisioning were designed many years ago. Differentiated Services (DiffServ) [7] and Integrated Services (IntServ) [8] were defined in Request for Comments (RFC) in 1998 and 1994 respectively, and IP networks QoS was mentioned for the first time in RFC 1006 [9] in 1987. Despite that, QoS provisioned traffic is still rather rare in ISPs' networks, and even if some QoS mechanisms are available in one domain, they are not really transferred to neighbouring domains.

The motivation for addressing end-to-end QoS is the heterogeneity of data networks currently interconnecting the users, which is seen as the biggest obstacle for QoS provisioning on a wider scale. The objective of the research described in this thesis is to investigate the possibilities for integration of QoS mechanisms in home, access, and finally core networks. It is a known fact that these networks are different in many aspects. Home networks are relatively small, they usually are a single entity from ownership perspective, and have multiple devices, which are quite different considering their capabilities. Additionally, these devices tend to join and leave the network frequently (both because they are switched on and off, but also carried in and out from the home network range). Access networks are usually owned by a number of ISPs. Various ISPs' networks are often technically different, but it is not unusual that also one ISP has different types of access links. Usually it depends on technologies available during roll-out, the distance between the central office and customer premises etc. The core of the network also is a mixture of technologies (e.g., SONET, DWDM, ATM, IP). Additionally, it carries significant amounts of data and due to that fact there is a tendency to simplify these networks and move traffic management towards the edges. Simpler core network components process less information about the forwarded traffic making the forwarding itself faster.

One could ask a question - can we count on a unified network management one day? It is hard to give a definitive answer, however most likely

the answer is: no. Different economical capabilities of different providers and customers will always allow faster upgrade to newer technologies to some, while others will stay behind with their legacy equipment.

The motivation for starting the investigation of QoS provisioning from home networks is twofold. First of all, since QoS in home networks has not been a very urgent issue, the work done until now might require supplementation. A relatively high bandwidth inside the home network, with many times lower bandwidth on the access side of the Home Gateway (HG), and a limited number of services available, did not call for much research and implementation effort in this area. Nevertheless, the situation in home networking has changed. With the Fibre to the Home (FTTH) roll-out, the proportion between access link capacity and bandwidth available in home network changes (both parts getting more equal) and the number of services delivered by ISPs grows. This brings more focus at user premises QoS. The second important argument for focusing on the home networks is coming out of already mentioned trend for placing network intelligence on the edges of the network. Initiating QoS signalling from a HG is an approach that can lift some processing burden from access nodes allowing them for more efficient switching, once the path is established. To allow home network nodes to perform signalling in the access part of the network some heterogeneity issues need to be addressed i.e., proper mapping functionality needs to be developed.

Besides the diversity in QoS signalling between different domains, there might also be multiple approaches to traffic management within a single domain. When this kind of heterogeneity is considered, one of the approaches to address this issue might be the use of a unified overlay network control plane. GMPLS can be seen as the protocol suite that attempts to bring different technologies under a common control and management umbrella, using different standardized extensions. This thesis also considers such an approach and provides analysis for including Passive Optical Network (PON) technologies in possibly end-to-end GMPLS controlled path.

Finally, it is important to consider things on a more general level. It is important to investigate the impact of certain QoS strategies using teletraffic theory. This allows to observe the relations between different parameters using mathematical models. These generic approaches might

be helpful when core networks are considered, as tests bed or detailed simulations are difficult or simply impossible to develop.

This thesis consideres various aspects of QoS provisioning in different domains of communication networks. It aims at addressing chosen issues of end-to-end QoS provisioning, outlining the possible integration of different technologies and concepts constituting today's and future network domains.

Structure of the Thesis

This Ph.D. study resulted in peer-reviewed journal and conference contributions [10–28]. The chapters of this thesis are based on a selection of them.

The remainder of this thesis is organized as follows: chapter 2 gives an introduction to home and access networks QoS concepts, and inter-domain mapping. In chapter 3, various home network QoS mechanisms available in Universal Plug and Play (UPnP) are discussed. A preliminary assessment of UPnP-QoS performance is presented based on analysis and simulations of chosen QoS establishment parameters. Chapter 4 considers the shortcomings and open issues of UPnP-QoS specification. It presents extensions to UPnP-QoS together with the results of their implementation.

Chapter 5 presents the work on merging QoS provisioning between different domains. Generalized Multi-Protocol Label Switching (GMPLS) and Resource ReserVation Protocol (RSVP) QoS mechanisms are described and the mapping between UPnP-QoS home and GMPLS based access is presented. Additionally, this chapter presents the idea of GMPLS Control and Managemet (CM) for PON networks. Chapter 6 discusses topics of reservation management and is more traffic engineering oriented. Resource sharing using a reduction factor is analysed with a single node, which is further used in open and closed queueing network analysis. Conclusions for the work presented in this thesis can be found in chapter 7.

Chapter 2

From Internet QoS to Home and Access QoS

Quality of Service (QoS) has been worked on for many years now. Despite this, it is still very unusual to have Internet Service Providers (ISPs) selling true QoS to their customers. This is because QoS is not easy to provide. Not only due to technical issues but also, or even mainly, due to political and business reasons. This chapter covers some of these problems and defines the scope of this thesis.

2.1 Network neutrality and QoS

Lately the discussion about network neutrality brought up the issues of QoS related packet inspection. Though the neutrality discussion covers mainly service differentiation, it is a source of quite vivid discussions. From a technical point of view differentiated QoS is the most straight forward to implement. At the same time QoS is rather something new for ISPs to sell to their clients and is something that requires cooperation with other operators, in particular if end-to-end QoS is considered. For these reasons some effort is required to understand how to perform traffic differentiation in order to have most of the actors benefit from the new service. From the ISPs' point of view, deploying differentiated QoS might help them to meet future video traffic requirements without as much infrastructure upgrade as it might be required otherwise. Additionally,

it might be a way to balance between different types of users - the heavy bandwidth consumers and the ones effected by them. It is also a chance for operators to differentiate themselves from competitors and be part of the innovation that was happening mainly through service providers [29].

The biggest challenge in wide scale traffic differentiation based QoS provisioning is coming from the issues connected with interconnecting different domains. ISPs today are not really sure how to interact with their peers. It also seems that not much will happen without a proper push from the regulatory side. Regulations might encourage building alliances between operators, which increases the probability of successful unified traffic differentiation in larger areas - possibly end-to-end QoS solutions can emerge.

2.2 Potential problem with Internet QoS

Besides the political reasons described above, there are many technical issues with large scale QoS. When Internet QoS is discussed the main models considered are Differentiated Services (DiffServ) and Integrated Services (IntServ). As far as unmodified IntServ is concerned, it is considered not scalable for large networks. This is due to the fact that the requirement for per-flow status is usually not feasible in case of thousands of flows running through core nodes. On the other hand there is DiffServ that with basic packet prioritisation is not causing scalability issues and schedules all packet belonging to a particular class in a certain manner. DiffServ, though technically quite straight forward to implement and favoured among the ISPs (at least what is visible from the neutrality debate), has its drawbacks. Firstly, according to [30] the cost of interdomain virtual leased-line IP service built on DiffServ is too high considering the benefits. It is also pointed out that simple DSCP-based traffic classification (e.g., leaky-bucket policing and priority queuing) is not sufficient. Secondly, its implementation can become cumbersome e.g., when class remarking and merging is considered [31].

Finally, there is an additional fact that causes many people to believe that Internet QoS is impossible, namely, the Internet was not built for QoS [32]. Its coexistence with PSTN and initially total separation from real-time services did not create strong QoS requirements. Since then the network has grown unimaginably (to roughly 30000 Autonomous

Systemss (ASs) and 180000 edge routers [33]) and tremendous revolution in services took place. However, the approach to forwarding packets did not change significantly. Obviously it has been a while since real-time applications' quality was susceptible for mistreatment in the Internet. However for some time already, parallel to service development and upgrades in transmission technology, allowed for responding to the growing demands with over-provisioning. While on one hand the efficiency of over-provisioning should grow with growing network size[1], on the other hand it might drop with the higher number of network domains [34].

2.3 Home Networking and QoS

Networking in the home environment is significantly different in comparison to networking in ISPs networks or in corporate environments. The differences between these networks are numerous. Firstly, it is the network size, home networks are usually rather small (though their growth is quite rapid). Since there is usually a manageable amount of network devices, and consequently traffic flows, some of the networking constraints are removed e.g., those related to scalability. Secondly, the installation and the management of home networks are usually performed by network users, while for other cases it is usually trained personnel that is handling networks' roll-out and maintenance. Another important factor that differentiates home networks is the traffic profile. Especially lately, the traffic in home networks is predominantly multimedia based, and it seems that this trend will continue. A short description of some home networking protocols is presented below.

2.3.1 Zeroconf

The need for enabling easy network configuration for home users was recognized early in the home PC era. The IETF Zeroconf Working Group was established in 1999. Their main objective was to enable the ease of use of home IP networks by:

- Allocating addresses without a Dynamic Host Configuration Protocol (DHCP) server (IPv4 Link-Local Addressing).

[1] Assuming capacity growth faster than an increase in the number of routers [34].

- Translating between names and IP addresses without a Domain Name Server (DNS) server (Multicast DNS).

- Finding services, like printers, without a directory server (DNS Service Discovery).

A number of documents were the outcome of the IETF Zeroconf Working Group, with RFC 3927 [35] probably being the most important. It describes how a host can automatically configure its address on ad-hoc or isolated networks. A number of implementations followed the initiatives for auto-configuration in home networks. [36]

2.3.2 Bonjour

Bonjour [37] is Apple's continuation of Rendezvous, and Apple's proposal for zero-configuration networking over IP. It covers the same three areas that IETF was addressing:

- addressing (allocating IP addresses to hosts) - based on randomly chosen and tested address.

- naming (using names instead of IP addresses in order to refer to hosts) - based on Multicast Domain Name Server (mDNS), where a device responses with its own address for requests with its name, Bonjour mDNSResponder daemon additionally relieved the service from interpreting mDNS messages once the service was registered on local host.

- service discovery (finding services on the network automatically) - mDNS query is sent out for a given service and a list of names of devices that host such a service is created.

Bonjour uses caching, suppression of duplicate responses, and exponential back-off with service announcement to reduce the network load.

2.3.3 IGRS

IGRS [38] communication system was developed to improve interoperability between the devices that are traditionally separated in three

domains: (a) computing (includes computers and peripheries), (b) consumer electronics (TV, HIFI, settop-boxes), and (c) communication (phones, PDAs). Its design is aiming at use simplification. IGRS defines: device discovery and grouping, message routing, device and service advertisement, identification and management, sharing mechanisms, and application profiles management. The IGRS specification places great emphasis on the concept of the IGRS Device Group, creating virtual groups using different criteria e.g., type of service or physical device properties. The creation of this "virtual device" i.e., composition of logical devices, aims at improving the efficiency and the simplification of resource management, by hiding the lower layer complexity.

2.3.4 Jini

Jini [39], is based on Java. The mechanisms it provides were designed to offer services over a network in an easy and fast manner.

Typically for a service discovery oriented protocol, the main features of Jini are: service registration (a service needs to be registered in order for a client to use it) and service lookup (enabling users to find a particular service). Additionally, it defines a service proxy object, which is a Java object specifying service capabilities and the code needed to use the service.

For automatic enabling and disabling of services, Jini uses portable source code and dynamic downloading. In Jini the stub code[2] used by the client, comes from the service the client wants to access. Jini obtains the stubs (proxy objects) using Jini Lookup Service. Since the Java code is essentially downloaded from the service itself, this approach makes the updates easier as a new version of the service interface can be downloaded on each service invocation (of course if required).

2.3.5 DPWS

Device Protocol for Web Services (DPWS) [40] was designed to fit the requirements of resource constrained devices into Web Services architectures. DPWS is a Web Services profile for plug-and-play networking between devices. The specification defines interoperability between differ-

[2] Code implementing an interface to a remote service present in the service client's address space.

ent resource constrained Web services allowing flexible client implementations [41]. It defines addressing, discovery, eventing, and description. In DPWS the stress is put on the compatibility with the Web Services. The following communication features are supported in DPWS [42]:

- DPWS-capable device discovery
- Messaging between DPWS-capable devices
- Web Service Definition Language (WSDL) based description of Web service
- Interaction with a service based on its description
- Eventing of Web service

2.3.6 UPnP

Universal Plug and Play (UPnP) [43] is a protocol suite that attempts to simplify the network establishment enabling seamless communication of devices. It has been defined by the UPnP Forum and is intended for home networks mainly. The UPnP suite defines six networking steps and sub-protocols, which are described below.

Addressing

UPnP uses IP addressing, and all devices should implement DHCP [44] client. For cases where there is no DHCP server available, a UPnP device should use the Auto-IP. If no valid DHCPOFFERs were received in a specific (implementation dependent) interval, the device sends Address Resolution Protocol (ARP) [45] probe to determine the availability of addresses. After configuration of the address, the device sends two gratuitous ARPs to ensure no ARP cache entries are left from previously registered devices. Within the home network, due to its character (i.e., users being more familiar with types of devices they own rather than their IP addresses), it is advised to use DNS [46, 47] to enable friendly names. The device manufacturer is responsible for ensuring the device's name is unique or for providing means for changing the name. [48]

Discovery

Discovery is the first step in UPnP networking (it follows Addressing which is referred to as step 0). UPnP discovery allows a device to advertise its services to a control point, and it allows the control point that is joining the network to search for devices of interest. UPnP discovery is based on Simple Service Discovery Protocol (SSDP) [49]. SSDP uses User Datagram Protocol (UDP) unicast and multicast to advertise services from a particular device. Advertisements are multicast on standard address and port (239.255.255.250:1900) and it has to be performed by every newly added device. The control point issuing the search message should receive the descriptions of devices matching the searched type via unicast messages identical to messages multicast by devices upon joining the network. [48]

Description

For interaction with UPnP device a control point in the network needs to retrieve the device's description. The description is pointed by the Uniform Resource Locator (URL) provided in a discovery message. The description is expressed in Extensible Markup Language (XML) and contains numerous information: vendor specific data, list of embedded devices or services, URLs for control and eventing, and presentation document (which similarly to device descriptions are in XML form). The description includes a list of actions and parameters or arguments for each action. [48]

Control

Based on the knowledge obtained during the description retrieval procedure, a control point can invoke actions on particular devices and their services. The control procedure is essentially based on the control point sending an action request to the device's service. Service then returns the action specific values, or in case of failures - fault codes. The control messages are sent to the control URL for the service of interest. The effects of this action may be reflected by a change in the state of a variable particular to a given action. Each service is responsible for maintaining its state table consistent - allowing the control point to obtain meaningful

information about the state of the service. [48]

Eventing

It is also possible for a control point to subscribe to information regarding the change of a certain variable. This subscription is referred to as eventing. Eventing frees the control point from the need to constantly monitor the state of the device or service, instead the service publishes the change by sending the event message. First event message contains the list of all evented variables. The source of the event i.e., the publisher can keep multiple control point updated regarding its status.

Presentation

UPnP device can also provide a more user friendly presentation of its current state via the Presentation protocol. A control point can access the presentation page from the presentation URL and load this page to a browser. This page depending on its capabilities can allow users to view the status of the device and services or enable their control.

2.4 Alternative approaches to QoS

2.4.1 Application level QoS

QoS in principle could be negotiated on the application layer. With a proper API it is possible to enable QoS requesting application itself to negotiate QoS with the network. As noticed in [32], DiffServ does not provide any direct possibility for QoS negotiation. Even if the application's requirement can be matched with Differentiated Services Code Point (DSCP), which should provide proper QoS, there are no guarantees that this service level will be obtained. When IntServ is considered, with the use of protocols like Resource ReserVation Protocol (RSVP), applications can learn about certain characteristics of the network. But then again, these applications have to be specially re-written and IntServ's scalability issues should be taken into account.

2.4.2 Web caching

Many years ago, potential problems of load growth and path latencies in the network brought the idea of web caching [50, 51]. Web caching is a possible solution for certain types of applications like Video on Demand (VoD) and similar. This approach is based on moving the content closer to the customer. It can improve users' perception of the service in a couple of ways. First, since the content is closer to the customer, the network latency is less visible from a user point of view. Additionally, network availability appears higher, because network outages are less likely to affect multiple sites [50]. Web caching has gained some popularity last years and exhibits very satisfactory results, making it a common QoS tool among content providers [32]. This solution unfortunately cannot improve QoS for multi-site applications like, telepresence, VoIP, etc. It also suffers from other issues related to maintenance of the integrity, use of cookies, and security [50].

2.4.3 Overlay QoS

Some ideas that try to separate the QoS provisioning from the underlying layer are presented in [52]. The authors propose QoS overlay that aggregates the flows and sends their traffic over *controlled load virtual links*, which should ensure a low packet loss if an aggregate consumes bandwidth within a certain range. The idea is based on packet loss calculation and the use of Forward Error Correction (FEC) and Automatic Repeat reQuest (ARQ) within the overhead bandwidth to ensure that the packet loss is below required level. The advantage of this approach is that it does not require the IP layer (assumed to be the underlying layer) to be neither DiffServ nor IntServ aware. On the other hand, it does not provide strict guarantees on loss boundaries. E.g., if a packet loss in the underlying layer increases (e.g., due to congestion), obtaining target packet loss might require higher overhead for a particular traffic aggregation. This in consequence, can cause other aggregates to suffer resource deficiencies. Some scenarios where trading throughput for loss and spacial bandwidth redistribution (basically distinguishing more and less important flows and distributing the losses accordingly), can be a motivation for the overlay QoS. Though one should be aware that the solution is not providing hard guarantees for QoS level.

2.5 Narrowing the scope

2.5.1 Reservations

In this thesis a predominant focus is placed on QoS mechanisms where a reservation of the resources is made. This applies to both: home domain where parametrized QoS in UPnP-QoS Architecture is studied, and access domain where GMPLS/RSVP is considered. Also generic teletraffic consideration of resource reservation is presented. Though this approach is criticised because of lack of scalability, it is the only way to provide hard guarantees for a level of quality, understood primarily by fixed throughput, bounded delay, jitter and low or none packet loss. After all, QoS on a particular path is as good as it is in the weakest part of the network. Solutions that do not perform resource reservations might not be suitable for a certain type of applications. As far as Differentiated Services QoS is good for bandwidth starving applications, it is quite inefficient for delay and jitter-sensitive real-time traffic [53]. Another potential issue with DiffServ is that is has been shown to give satisfactory results when premium traffic accounts for a minor part of the total load. Historically the premium was considered to be a business critical traffic and realtime traffic like VoIP and interactive Video. The popularity of these types of applications is growing. Cisco prognoses that as much as 90% of future Internet traffic will be video, with significant share of interactive traffic [54]. This would mean that historically premium traffic might become a predominant in the total traffic, making DiffServ a questionable solution.

2.5.2 Focus on Home and Access

The research conducted in this thesis might be seen as a result of a certain trade-off. On one hand, it is investigating the resource reservation (with its already mentioned scalability issues), which can be seen as the ultimate QoS mechanism, with possibility for providing hard guarantees. At the same time is constitutes a quite complex solution with signalling protocols and queueing mechanisms. On the other hand, when the "geographical" scope of the research is considered, it is limited mainly to home and access networks. There are numerous reasons for this approach. First of all, as mentioned already, there are many people who

do not believe that the Internet QoS will ever be possible, and it is true that international nature of the Internet makes it difficult to set common QoS mechanisms. This is the primary reason for restricting the focus on home and access QoS and on the interaction between those domains. Secondly, home QoS is becoming needed and might have a big impact on the QoS provisioning in access networks. The need for QoS provisioning is coming from a growing variety of services offered to home users via a single data link, and a parallel growth in capacity of access links removing the bottleneck at the home gateway. The potential change in management of the access networks that is caused by home QoS architectures, is related to the trend of placing the intelligence of the network on its edges. With the use of home QoS mechanisms it is possible to place the intelligence of the network extremely close to the traffic source or destination. Considered in this thesis UPnP-QoS allows the request for the QoS in the home network to be originated by the UPnP-QoS aware application. As mentioned previously, resource reservation from the application layer requires API enabling interaction with the network. While the popularity of RSVP within home application/devices is rather low, the situation in this part of the network looks better for Digital Living Network Alliance (DLNA)/UPnP. This is why it seems more natural to start the reservation with UPnP-QoS request and allow this request to be translated for the need of a reservation in the access network. Of course the proper mapping needs to be performed, and the considered Home Gateway (HG) needs to be both UPnP-QoS and RSVP compliant.

Chapter 3

QoS in home Networks - UPnP-QoS Architecture

This chapter is based on the work presented in [10, 15, 17].

3.1 Introduction

Providing QoS within home networks is gaining attention when automated and intelligent homes are considered. Similar views on the network control and management might also be seen in small office environments. As indicated in previous chapters, this increased interest in home network QoS is mainly caused by the growing data traffic in home networks and diversity of traffic types with clear differentiation between the importance of particular traffic flows. At the same time, there is a great emphasis on introducing a management system that can handle the dynamic character of a home network, where devices leave and join the network frequently. Naturally, service based platforms are often a choice for organizing and controlling the described networks. There is a number of protocols designed for dynamic service discovery that can be used for establishment of home network: UPnP [43], DPWS [40], Bonjour [37], IGRS [38], Jini [39]. While Bonjour does not explicitly consider QoS, Intelligent Grouping and Resource Sharing (IGRS) and Jini are more focused on the end devices' resources than on the network's resources, UPnP (especially with its QoS Architecture) and DPWS are

clearly defining network QoS mechanisms. The scope of listed protocols is usually quite broad with emphasis on device/service discovery (as described before mainly due to dynamic character of the home network). Nevertheless this chapter concerns mainly the chosen QoS provisioning mechanisms, namely the resource reservation procedures, keeping in focus the context of home networking. UPnP together with its QoS Architecture specification provides a good environment for the evaluation of signalling procedures in service based architecture. That is why, in the remaining part of this chapter, only the UPnP-QoS Architecture [55] will be considered and the analysis will be based on its signalling model. However, the analyses made here are generic enough that they could be used for any QoS architecture where the resource reservation procedure is similar (e.g., DPWS). Some evaluation of the UPnP-QoS framework was done in [56] where the authors concentrate on performance in WLAN environment not really focusing on QoS level within different classes, whereas here it is shown how the UPnP-QoS Architecture reservation procedures differentiate flows depending on defined importance.

The remainder of this chapter is organized as follows. Section 3.2 outlines the UPnP-QoS Architecture components and signalling. Section 3.3 presents the analytical approach towards resolving chosen QoS setup parameters. Section 3.4 describes the model developed for simulations, while section 3.5 addresses the simulations results. Section 3.6 treats second version of the model used for the UPnP-QoS evaluation with devices' performance based on measurements from Multimedia over Coax Alliance (MoCA) devices [57]. Additionally section 3.7 outlines how UPnP-QoS fits together with different queueing disciplines in considered home network. Finally, a summary of the chapter is presented in section 3.8.

3.2 Modelling UPnP and In-home QoS

UPnP is usually used in a network where multiple devices and services with various requirements share the resources. For such a network, the introduction of QoS functionality seems to be natural. In [58] some extensions to the UPnP protocol were proposed, which indicated a need for further development of new functionalities. That is why the UPnP Forum (the initiative behind UPnP) defined the UPnP-AV Architec-

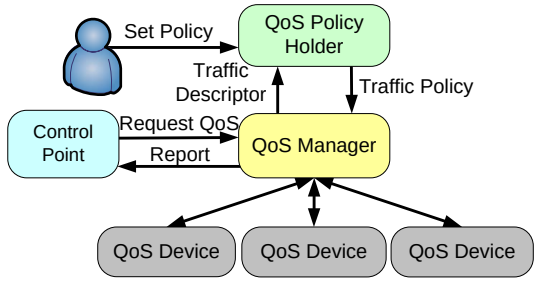


Figure 3.1: UPnP architecture

ture [59] and UPnP-QoS Architecture. While the first is destined for describing interaction between audio/video appliances, the second is more generic and describes the interaction of UPnP-QoS framework services that would allow QoS provisioning in home/office networks. The following sections describe the signalling procedures of UPnP-QoS Architecture in accordance with UPnP-QoS Architecture version 3 [55].

3.2.1 UPnP-QoS Entities

The UPnP-QoS entities and their relations are depicted in Fig. 3.1. The Control Point (CP) is an instance that has knowledge of the source and destination of a particular flow and the Traffic Specification (TSpec) of the content. It is not a separate UPnP module as such. CP sends the information to the QoS Manager (QM) that communicates with the rest of the services/devices on the network.

QM [60] is the coordination unit responsible for requesting, updating and releasing QoS assigned to various traffic streams. After receiving the request from CP it will be able to obtain and process traffic policy or policies from the QoS Policy Holder (QPH). Whether QM requests traffic policy or a list of policies depends on the QoS mode, a single traffic policy is requested for prioritized QoS setup, while for parameterized QoS setup, determination of properties of blocking flows will require obtaining a list of traffic policies of these flows. Further, QM passes admit/release requests to QoS Devices (QDs) that are on the path of a flow. The QPH [61] is responsible for providing the traffic policies to requesting QM that provides the Traffic Descriptor as input parameter identifying

the flow that the policy is requested for.

The QD [62] service resides on a source, destination or intermediate node of a particular flow. QD is administering its resources and reporting the state according to its configuration set by QM. QD is defined as responsible for providing proper network resources to the traffic flows that it accommodates. The specification considers some Layer 2 technologies and mapping of UPnP parameters to lower layer specific parameters. In work presented here the administration of the resources within the device model was performed on a certain level of abstraction. This approach allows for later specification of mapping mechanisms that could be used with multiple Layer 2 technologies.

The UPnP-QoS Architecture defines three types of QoS provisioning: prioritized, parameterized, and hybrid. Prioritized QoS is a default approach and means end-to-end traffic prioritization. Prioritization is performed based on the policy stored in the QPH. Parameterized QoS requires resource reservation on the entire traffic path, if not all segments in the network support this type of QoS, the attempt of its establishment will fail. Hybrid QoS admission can take place for situation when some of the segments on the flow's path are not supporting parameterized QoS and CP allows the use of prioritized QoS on those segments. [55]

UPnP-QoS allows for signalling a priority of a particular flow by two numbers. The first of those is User Importance Number (UIN) and it is used to indicate the importance of the traffic source (this can refer to an application or a device). UIN is used on the UPnP-QoS signalling layer (e.g., for deciding on the preepmtion). The second priority indication considered in the specification is Traffic Importance Number (TIN) that is specifying the importance of the traffic itself and if possible should be considered by lower layer functionality e.g., Layer-2 aware schedulers.

3.2.2 Signaling in UPnP-QoS

The analysis in this chapter mainly considers UPnP-QoS signalling during establishment of parameterized QoS. The interaction diagram for reservation is presented in Fig. 3.2. Its upper part shows the reservation for a case without preemption, which is a case where there are enough available resources or where preemption is not requested. The diagram as a whole (above and below the dashed line) present the interaction

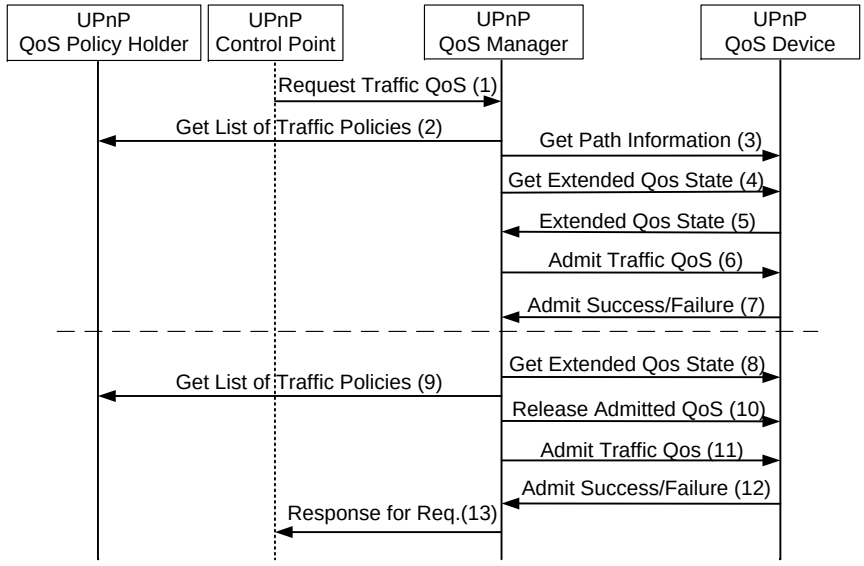


Figure 3.2: Interaction diagram for Traffic QoS request with preemption

between the UPnP-QoS services when preemption is enabled. [55]

The basic procedure for traffic QoS establishment (see Fig. 3.2) starts with CP's QoS request for a given flow sent to QM (1). The request contains the Initial Traffic Description and Resource parameters, which define flow's basic parameters and resources that are requested. Later QM, based on the source and destination addresses contained in the Initial Traffic Descriptor, determines the path for the flow and decides which devices need to be configured for an incoming traffic (2). This is followed by determination of the state of QDs with Get Extended QoS State action (3), in response the QDs provide information about their capabilities and current state (4). Afterwards, the QM will invoke the Admit Traffic QoS action (5). [55,61]

In case the attempted reservation fails and CP requests preemption, the QM will continue the reservation procedure. The QM will request from the QDs the information about the blocking flows using a second Get Extended QoS State request (6). Once the QM has knowledge of blocking flows it can send the Get List of Traffic Policies request to the QPH for the list of traffic policies (7). Based on obtained policies the QM

can make decision if and what should be preempted. After determining the flows for preemption the QM tries to: release sufficient resources (8) and admit the newly requested flow again (9). Normally, preemption will take place in the situation where the requested resources are not available on one of the network devices. However, some of the resources are occupied by the flows that according to the traffic policies are of the less importance comparing to the newly arriving flow. The specification does not define details for the process of choosing flows to be released in case there are multiple candidates for preemption. Next chapter of this thesis addresses this issue by proposing a few preemption algorithms and analysing their performance in a home network environment.

3.3 Analysis

As for the performance analysis the focus is on two major aspects of the reservation procedure that influence the overall performance and quality of network architecture, namely: setup time and rejection ratio.
Below the analytical approach for determining these parameters is presented.

Notation:

t_{tot}	Total QoS setup time
t_{α}	Time required for the first QoS setup attempt
t_{check}	Time to determine the cause of reservation blocking
t_{γ}	Time for release and readmission
p_{β}	Probability that the flow cannot be admitted due to lack of resources (blocking probablity)
p_{γ}	Probability of causing pre-emption
t_{rtq}	Time required for Request Traffic QoS
t_{gltp}	Time required for Get List of Traffic Policies
t_{gpi}	Time required for Get Path Information
t_{eqs}	Time required for Get Extended QoS State
t_{atq}	Time required for Admit Traffic QoS
t_{ar}	Time required for Admission Success/Failure
t_{rel}	Time required for Release
D_n	Number of devices in the network
D_p	Number of devices on the QoS path
t_{pd}	Propagation delay
t_{dpd}	Device processing delay

UPnP-QoS setup time has three distinguishable phases and can be denoted as:

$$t_{tot} = t_{\alpha} + p_{\beta} \cdot t_{check} + p_{\gamma} \cdot t_{\gamma}. \tag{3.1}$$

First attempt setup time is defined as:

$$\begin{aligned} t_{\alpha} \quad = \quad & t_{rtq} + t_{gltp} + d_p \cdot t_{gpi} \\ & + d_p \cdot t_{eqs} + d_p \cdot (t_{atq} + t_{ar}). \end{aligned} \tag{3.2}$$

Time required for checking the possibility for the pre-emption (i.e., the state of the devices) is defined as:

$$t_{check} = d_n \cdot t_{eqs} + t_{gltp}, \tag{3.3}$$

while pre-emption time is defined as:

$$t_p = d_p \cdot (t_{rel} + t_{atq} + t_{ar}). \tag{3.4}$$

Where d_n for sequential QoS establishment is equal to D_n, while for parallel QoS establishment $d_n = 1$, d_p for sequential setup procedure is equal to D_p, and $d_p = 1$ for parallel QoS setup. t_{rtq}, t_{atq}, and t_{ar} are equal $t_{pd} + t_{dpd}$, and remaining time components are $2 \cdot t_{pd} + t_{dpd}$. In this section the parallel setup is considered (i.e., $d_n = 1, d_p = 1$), and the time required for processing the UPnP message within devices is neglected (i.e., $t_{dpd} = 0$). Later, section 3.6 presents the analysis for experimentally obtained t_{dpd}, which differs from 0.

Both p_β and p_γ seem to be non-trivial to derive. Intuitively the blocking probability is increased with offered traffic ($p_\beta \propto A$). On the other hand, the probability of high enough priority to cause preemption will be inverse proportional to offered traffic and proportional to flow priority ($p_\gamma \propto priority/A$).

For derivation of p_β it is enough to notice that at this stage of flow admission the priority is not considered. The flow tries to access the free resources and the priorities of flows already in the system does not matter. This means that the collective offered traffic should be considered and Erlang-B formula may be used:

$$\begin{aligned} p_\beta &= E_n(A) = \\ &= \frac{\frac{A^n}{n!}}{1 + A + \frac{A^2}{2!} + ... + \frac{A^n}{n!}}, \end{aligned} \tag{3.5}$$

where $A = \sum_{i=1}^{p} A_i$, A_i being the traffic offered by priority i.

For calculation of p_γ, first the problem described in [63] and [64] and later generalized in [65] is considered for obtaining a blocking probability for prioritized preemptive single rate traffic. For p classes of independent Poisson traffic sources, the r_i is defined such that $1 \geq r_1 \geq r_2 \geq ... \geq r_i \geq ... \geq r_p \geq 0$, is denoting the proportion of offered traffic with a

particular priority or higher. With the assumption that higher priority traffic always can preempt lower priority flow, the blocking probability of priority i is given by Erlang-B formula for offered traffic Ar_i:

$$B_i = E_n(Ar_i). \tag{3.6}$$

That is due to the fact that higher priority traffic does not see lower priority flows. Knowing B_i it is easy to derive probability of preemption p_γ, it is simply:

$$p_\gamma = p_\beta \cdot (1 - B_i). \tag{3.7}$$

This leads to total time for QoS establishment for priority i flow:

$$\begin{aligned} t_{tot}(i) &= t_\alpha + p_\beta \cdot t_{check} + p_\beta \cdot (1 - B_i) \cdot t_\gamma \\ &= t_\alpha + p_\beta \cdot (t_{check} + (1 - B_i) \cdot t_\gamma). \end{aligned} \tag{3.8}$$

Finally, $t_{tot}(i)$ can be written as:

$$t_{tot}(i) = t_\alpha + E_n(A) \cdot (t_{check} + (1 - E_n(Ar_i)) \cdot t_\gamma). \tag{3.9}$$

Considering the rejection ratio, equation 3.6 can be used directly.

In fact, jobs arriving in this scenario can request a uniformly distributed amount of resources. That makes this problem much more complex and simulations are used for verification of the protocols performance. Below (section 3.4) the model is described, and this is followed by simulation results and their analysis in section 3.5.

3.4 Model

Developed simulation model consists of all the UPnP-QoS architecture elements as presented in Fig. 3.1. It is assumed that the QM, QPH and CP functionalities are implemented in a single node, issuing the QoS requests. This node (e.g., a home gateway) is interconnected with three end-QDs by an intermediate QD with switching functionality. All the links in the model provide 70 Mbps full-duplex connectivity. The CP generates requests in exponentially distributed intervals with a mean value used as a parameter of the simulations. Each device manages

its state divided into 10 classes, equivalent to UIN. The priority of each flow i.e., the class-number is assigned uniformly between 0 and 9. The resources requested by flows range between 5 and 45 percent of class capacity (each class have access to an equal share of the total link capacity). The pair of source and destination is randomly selected. Reservation holding time is exponentially distributed with the average of 120 seconds. The arrival rate of QoS requests is adjustable and the results are present for request rates between 0.1 to 0.8 requests per second - equivalent of 25 and 200 percent of network capacity, where offered traffic is calculated using equation 3.10.

$$A = \frac{\lambda}{\mu} \cdot d, \tag{3.10}$$

where λ is arrival rate of a Poisson process, μ is a service rate i.e., inverse mean service time, and d is the number of channels (amount of resources) in multi-rate system.

The outbound interface is UPnP-QoS managed by the bookkeeping of interface resources, which means once a request for a new reservation arrives, the QD verifies if it is possible to accommodate this reservation in particular class by verifying if:

$$\sum_{ID=1}^{n} Res_{ID} + Res_{new} \leq Res_{total}. \tag{3.11}$$

Where Res_{ID} are the resources occupied by established earlier flows with a particular ID (flow identifier), Res_{new} are the resources requested for a new flow, and Res_{total} equals to the total amount of resources available for each of ten modelled classes.

3.5 Simulations

During the modelling and simulation activities two earlier described aspects of the reservation procedure were considered (i.e., setup time and rejection ratio). First, the reservation setup time within different classes of service is investigated and second, the rejection ratio of arriving reservation request is considered. Fig. 3.3 shows that the average setup time for higher priorities reservations is higher. This is an expected tendency,

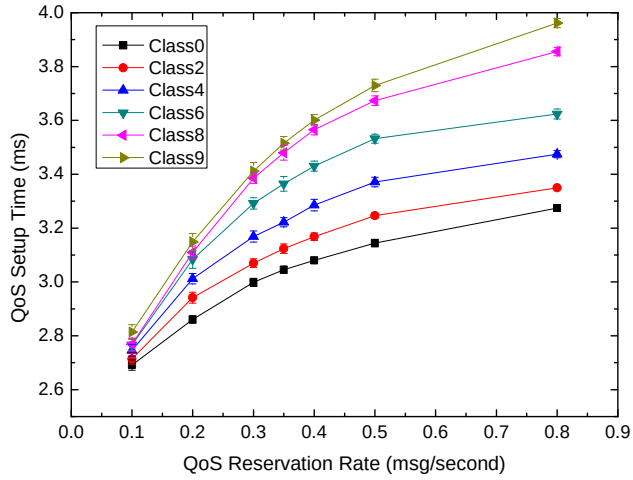


Figure 3.3: Setup time for flows of different priority in function of traffic QoS request message generation rate

simply because, as indicated previously, the reservation with preemption takes longer and this kind of reservation is less likely to happen for low priority traffic. Another observation is that this tendency does not change for growing traffic QoS rate. The graph also shows that higher generation rate causes extension of setup time, which increases around 20% for low priority flows and 40% for high priority flows. Higher impact on the setup time of high priority flows can be explained by the fact that preemption is occurring more often for higher message generation rates and mainly affects the higher priority traffic flows which cause preemption more likely than the low priority reservations (lower priority can not cause preemption that often as flows occupying resources are less probably to be of lower priority, especially for high reservation generation rate).

Fig. 3.4 presents rejection ratios for flows with different priorities measured as a number of reject notification for a particular priority over total number of notifications (rejections and acceptances) received. The results of the simulation clearly show that the ratio of rejected messages for lower priorities are higher. One can also see that the rejection ratios for all the priorities grows with growing rate of message generation i.e., offered traffic. Analysis of the data also shows that the reservation rejec-

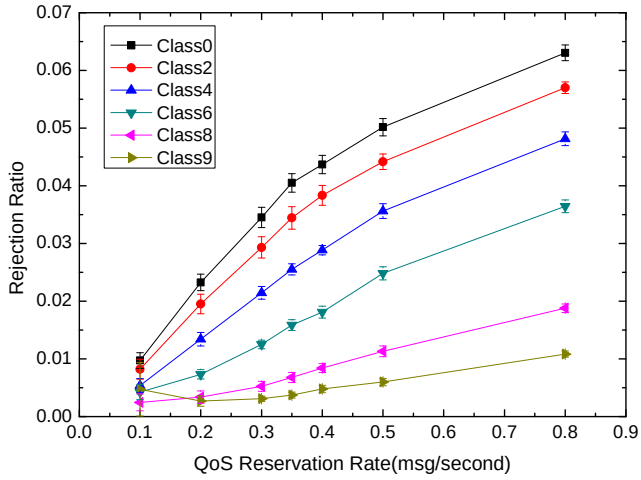


Figure 3.4: Rejection ratio for different priority flows as a function of the flow initiation rate

tion ratio for lower generation rates is well distributed between classes, providing good separation between different priorities.

Additionally, the results for very high load are presented in Fig. 3.5. For such loads p_β will tend to 1 ($\lim_{A\to\infty} p_\beta = 1$). p_γ for low priorities will relatively fast lead to 1, while for the highest priorities it will stay close to 0 (it would tend to one for extremely high loads not considered here). That means that for high loads (but not extreme that would cause preemptions in priority 9 flows) the setup time for high priority traffic should be:

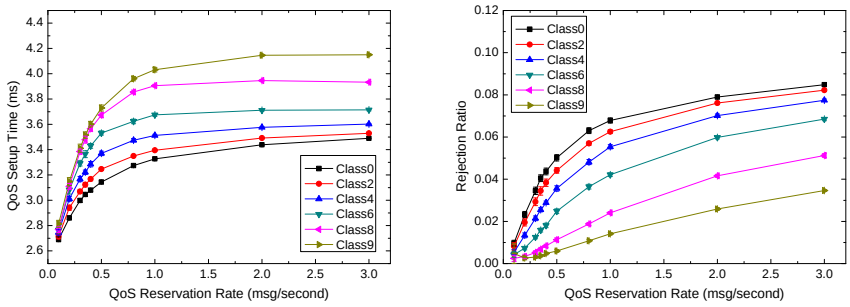
$$t_{tot} = t_\alpha + t_{check} + t_\gamma, \tag{3.12}$$

and not considering message processing time it is equal to 4.3 ms (see Fig. 3.5 (a)). For low priority traffic at high loads the setup time could be calculated from:

$$t_{tot} = t_\alpha + t_{check}, \tag{3.13}$$

which without processing delay, should tend to 3.6 ms. These results are confirmed by the Fig. 3.5 (a).

Another noticeable fact from Fig. 3.5 (b) is that lower priority rejection ratios seem to converge at the higher request rates. That can be



(a) (b)

Figure 3.5: Measurement of Setup time (a) and Rejection ratio (b) of different priority flows as a function of extended range of flow initiation rate

explained by the fact that at high generation rates devices are accommodating almost exclusively flows with priority (UIN) 9, and almost all lower priority flows are rejected. All the figures present a mean value with 90 percent confidence intervals.

3.6 Model and Simulations for MoCA devices

The model presented in previous sections was extended with the parameters obtained from measurements on the MoCA devices. The original model does not consider the time required for the XML message processing within the device (it was considering only the delay connected with queueing and propagation). As presented in Table 3.1, different messages are processed in different time. Incorporating these data into the model presents more realistic results for the MoCA devices. However, in principle it is hard to extrapolate this measurement for other devices as parsing time is very much dependent on the processing capabilities in the device (which was a motivation for not including it in a generic UPnP-QoS Architecture evaluation presented in section 3.4).

3.6.1 Model description

Presented here MoCA adapted model consists, similarly like the original model, of the elements presented in Fig. 3.1. In the MoCA model the requests are uniformly distributed between four priority groups. The

Table 3.1: Invocation times, i.e., response time and parsing for UPnP QoS Device on MoCA implementation(I) GPI: GetPathInformation, (II) GEQS: GetExtendedQoSState, (III) ATQ: AdmitTrafficQoS, and (IV) RAQ: ReleaseAdmittedQoS

MoCA node	GPI	GEQS	ATQ	RAQ
Network Coordinator	25 ms	110 ms	429 ms	72 ms
parsing	7 ms	18 ms	-	-
non-Network Coordinator	18 ms	110 ms	908 ms	120 ms
parsing	7 ms	19 ms	-	-

amount of resources requested are uniformly distributed in a range of values between 10 and 40% of the bandwidth assigned for each class. The simulation time is 200 minutes with a 25 minutes warm-up period. The QD response times used in the model are based on the values with the Network Coordinator in the MoCA network (see Table 3.1).

3.6.2 Simulations

The motivation behind the performed simulations is to verify the QoS differentiation for requests with different priorities in a dynamic scenario where the message processing time within the QDs is considered.

Fig. 3.6 shows the QoS request rejection ratio in one of the four classes. The results are similar to those presented for a generic case, which indicates the expected i.e., that parsing time has no impact on the level of separation between QoS granted to different classes.

Fig. 3.7 presents rejection rate, where it is also visible that lower priority classes are rejected on more regular basis.

Fig. 3.8 presents the average MoCA QoS setup time results for different priorities in a range of QoS request rates. This characteristic is slightly different than the setup times presented in Fig. 3.3. First of all the setup time in this case is considerably longer (as expected). It is important though, that for the selected range of reservation generation rates, the setup time is within reasonable range of approximately one second. The increase of the setup time (similarly as in previous section) caused by preemption is reflected in different setup times across request priorities, as a high priority request is more likely to cause the preemption. The results also show that an increase of the CP's request rate causes the extension of the time required for QoS establishment for all

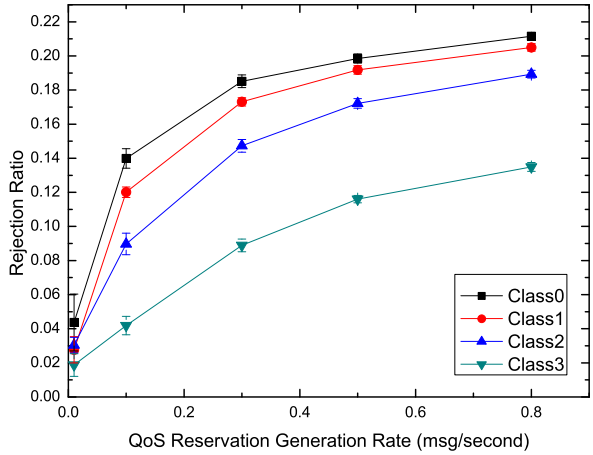


Figure 3.6: Rejection ratio for different priority flows as a function of the flow initiation rate

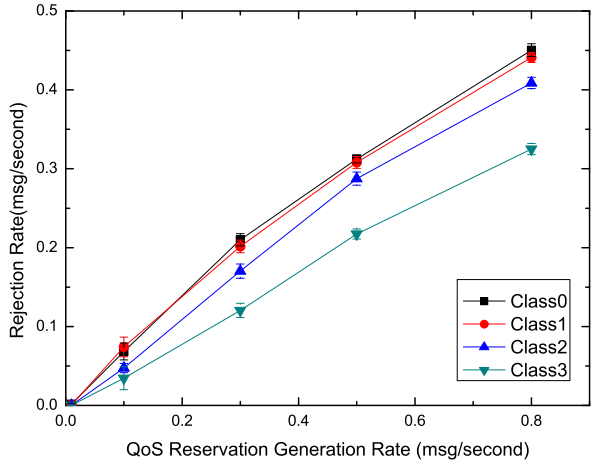


Figure 3.7: Rejection rate for different priority flows as a function of traffic QoS request message generation rate

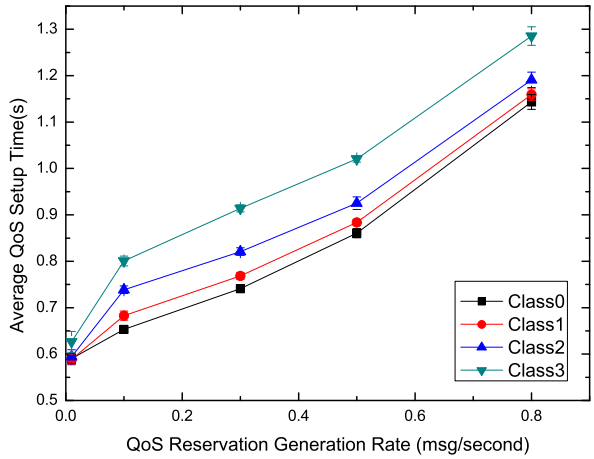


Figure 3.8: Setup time for flows of different priority in function of traffic QoS request message generation rate

priorities, as the preemption probability caused by all priorities grows.

3.7 UPnP-QoS and queuing

This section treats the QoS of traffic flows on a data plane layer. The work presented here is aimed at finding out how provisioning QoS on higher layer (i.e., application layer) using UPnP-QoS is fitting together with different queueing techniques. The motivation for this work is to verify if it is possible to opt for simpler queuing techniques in devices that implement resource control using UPnP-QoS.

3.7.1 Model details

The model used for work presented in this section similarly like in proceeding sections is a representation of the UPnP-QoS Architecture in a parameterized setup and contains logical entities as presented in Fig. 3.1. The topology of the network used is presented in Fig. 3.9.

Reservation mean holding time is 120 seconds, and the average reser-

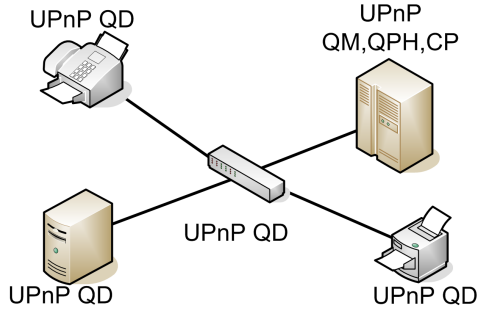


Figure 3.9: Topology of UPnP-QoS managed network for delay measurements

vation consumes 25% of resources available in the particular queue. The inter-arrival time for requests is exponentially distributed with the average specified for a particular simulation run (0.1 - 3 requests per second). The UIN is uniformly distributed and grouped in 10 classes (from 0 to 9). The average packet size is 512 bytes. Devices might implement First In, First Out (FIFO) queue or strict priority queueing, where unless higher priority queues are empty the lower priority queues are not serviced. Also the situation where only some of the devices (typically the switching device in the network) are equipped with priority queueing, while end-devices are FIFO enabled, is of interest. The flow's assignment to a particular queue (Layer 2 priority i.e., TIN) is uniformly distributed. For multi-queue devices each interface is composed of 8 queues, and each flow is assigned to one of them. As described earlier, two levels of priority can be discussed. One on the signalling level, where UIN determines which UPnP-QoS requests are rejected or accepted. The second level of priority is queue related and determines how the queues in each interface are serviced during the time of congestion. The second level of priority is related to TIN.

3.7.2 Simulation Results

Simulations performed were aiming at delay analysis for different approaches to queuing and verification if simplified queuing in the home networks can be supplemented with application level control using UPnP-QoS. The analysis was performed in order to assess the improvement in

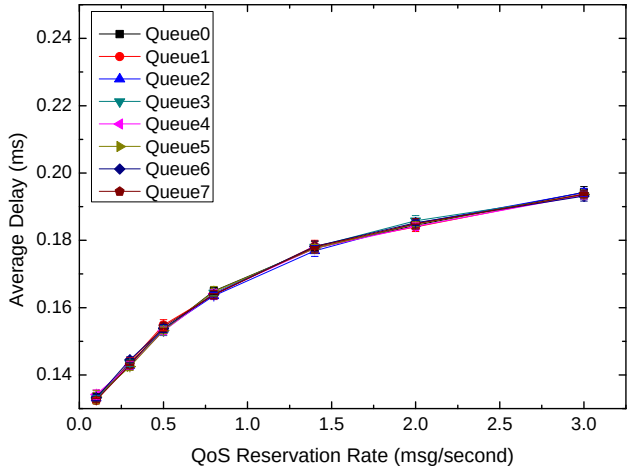


Figure 3.10: Average end-to-end delay for different packet generation rates with FIFO queuing in all devices

the end-to-end delay characteristics. First, delay characteristics presented consider a case where all end devices and HG implement simple FIFO queuing. The second simulation shows the results for all interfaces based on priority queuing. Finally, the third scenario presents the results for a case where the end devices are equipped with FIFO queue and HG scheduler provides strict priority. It is important to point out that for all devices and interfaces in all the scenarios, UPnP-QoS resource administration is taking place. Devices control and report the state of eight virtual queues whether they are implemented (here as priority queues) or not (for cases where FIFO queue is described).

The results of the first scenario (Fig. 3.10), which are treated as a base line, show how UPnP based QoS provisioning can limit the maximum packet delay. The initial growth of the delay with growing reservation load is very limited once the resources are exhausted and the QM starts to perform limited admissions. Fig. 3.10 also clearly shows that prioritization that takes place on the UPnP-QoS level will not affect delay characteristics, and flows in all priority classes will experience the same delays. The priority that is considered by the UPnP QM is taking place only on signalling/control plane and is strictly UIN related. The packets that are generated with different UINs and TINs will eventually be

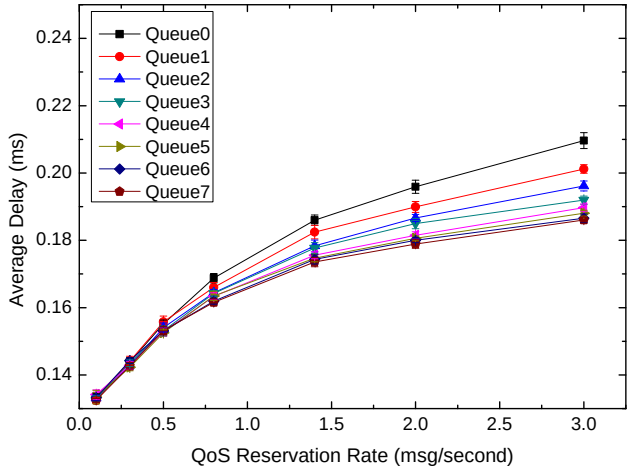


Figure 3.11: Average delay for different packet generation rates with FIFO queuing on end devices and priority queuing in GW

queued in the same FIFO queue and will experience the same delays. Here the benefits from deploying UPnP-QoS are limited to admission control, which will limit the queuing delay as a consequence of resources exhaustion.

Once UPnP-QoS gets "support" from the lower layer in the form of multiple queues that packets can be queued in, the benefits of using TIN can be noticed. For a case where all the end devices are equipped with a FIFO queue, and the UPnP-QoS enabled HG uses priority queuing, Fig. 3.11 show that very good separation of delay experienced by traffic belonging to different classes (here understood as different TINs) can be obtained using described queuing.

For the case where all the interfaces in the modelled network implement priority queuing (see Fig. 3.12) further improvement is visible (in sense of lowering delay of high priority flows), though the improvement factor is not significant.

3.8 Summary

The modelling discussed in this chapter shows that UPnP-QoS Architecture is capable of providing different levels of QoS depending on the

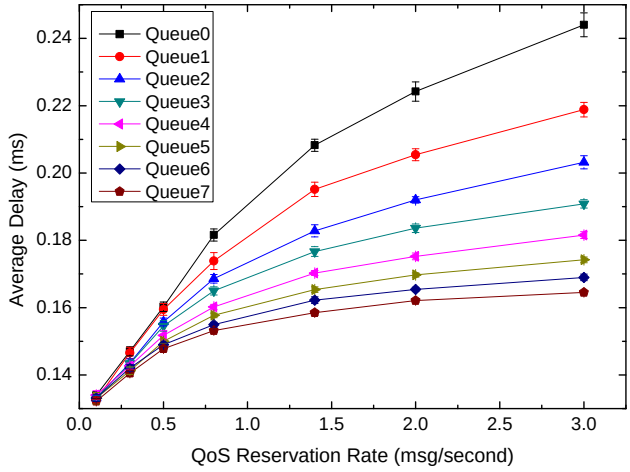


Figure 3.12: Average end-to-end delay for different packet generation rates with all queuing priority based

flows importance and user priority. This is best shown by parameters like rejection ratio and rejection rate that show that a higher importance number causes flows to be rejected less often. On the other hand, one has to be aware that higher priority flows have on the average higher setup times. Despite the reasons for this might be obvious, i.e., higher priority is more often causing preemption, which extends the setup time, it is still not desired, as usually a traffic with higher priorities should be serviced with better quality. One can argue that extension of setup time that in consequence avoids rejection is a fair solution. The setup time might not be of the highest importance, in some cases a small delay at the beginning of the traffic flow is not significant comparing to later in-time packet delivery.

UPnP-QoS signalling is well defined and performs well even using the simplest – sequential reservation and preemption approach (meaning no parallel resource management is performed). However, it is also worth noticing that the full specification of the UPnP-QoS Architecture is quite heavy, and the signalling overhead could be limited. On the other hand, this overhead might not be an issue for the protocol that is mainly intended for private networks, where traffic volumes are high and bandwidth price usually is not a problem.

When Layer 2 issues are considered, a described delay analysis was performed mainly in order to determine the need for advanced queue mechanisms with consideration of flow's priority. The results were aimed at the assessment of the delay reduction for high priority flows comparing strict priority queuing to simple FIFO queue. The results show straight forward benefits from the implementation of priority based queuing. On the other hand one could argue that 40 μs improvement in packet delay does not justify the need for priority queueing. The deployment of the UPnP-QoS Architectures alone with its resource and admission control, can preserve QoS well enough even for a case where interfaces have simple FIFO queues implementations. Of course the analysis were performed for small home network and benefits from priority queueing would be more visible in a larger environment. The overall recommendation could be that using FIFO in end device is sufficient, while advance queueing mechanisms in network components can be beneficial for packet delay characteristics, especially with a growing network size.

Chapter 4

Extending UPnP-QoS Architecture

This chapter is based on the work presented in [14,19,21,27].

4.1 Introduction

This chapter covers proposals for the extensions of the UPnP-QoS Architecture. As the first proposal, analysis and verification of lightweight preemption algorithms are presented. This is followed by the introduction and usability verification of a new UPnP-QoS service, which addresses the problem of UPnP-QoS non-compliant devices. Both extensions are verified through simulations using OPNET [66].

UPnP-QoS Architecture provides a good environment for evaluation of preemption procedures. In the remaining part of this chapter only UPnP QoS Architecture [55] is considered, and the analysis of preemption algorithms will be based on the UPnP-QoS signalling model. Nevertheless, analysis made here, similarly like in the previous chapter, are generic enough that they could be used in any QoS architecture where preemption is possible and managing entities are capable of determining policies of existing and incoming QoS requests.

The remainder of this chapter is organized as follows. Section 4.2 treats the preemption basics, next in section 4.3, a short analytical overview is given. In section 4.4 the preemption algorithms for UPnP-

QoS are presented. This is followed by preemption simulations and results in section 4.5.

In section 4.6 the Network Based Control Point is described. Next, in section 4.7 the automatic flow classification is treated, and its introduction in the UPnP-QoS model is described in 4.8. Section 4.9 covers the simulation and results for NBCP.

Finally, section 4.10 presents the summary of this chapter.

4.2 Preemption algorithms

Preemption (as mentioned in section 3.2) is a procedure that allows admission of a new traffic flow even in a case of insufficient amount of free resources. When a managing entity decides that the arriving traffic is more important than one (or a group) of the flows that already occupies some resources, it can release these resources and at the same time decline the previously granted QoS (usually equivalent of degrading the QoS to Best Effort). The preemption algorithms described in the literature [67,68], and [69] are aimed at the optimal (or suboptimal) solutions, minimizing rerouting, number of preempted flows and their priority. When centralized preemption is considered, the authors of [68] show that the problem is NP-complete. In home networking not all of listed above parameters are of high importance. E.g., rerouting usually is not a problem as home network topology is usually quite simple and there will not be many alternative routes, actually the topology is so simple that it is reasonable to make per interface decisions. When it comes to traffic priority and number of preempted flows these are parameters of bigger importance and they will be studied in this chapter in more details. Some studies like [70] consider a random selection algorithms showing that the optimal and suboptimal algorithms are outperforming the random selection. However, sometimes the latter achieves comparable results with much lower complexity. It is also important to mention that limited processing power in the home network justifies the focus on lightweight algorithms with low computing complexity and implementation effort. In this chapter three lightweight preemption algorithms are presented, they are designed to fit with general home network topology and processing power capabilities, at the same time being compatible with UPnP-QoS Architecture. Later also brief description of combining

different preemption algorithms is presented.

4.3 Analysis

In order to discuss preemption probability the system that was described in 3.3 can be considered. Again, using $1 \geq r_1 \geq r_2 \geq ... \geq r_i \geq ... \geq r_p \geq 0$ for denoting the proportion of offered traffic with a particular priority or higher. The preemption probability of a reservation with ith priority is:

$$p_{pree} = \frac{B_i - B_{i-1}}{1 - B_i} \cdot \frac{r_{i+1}}{r_i - r_{i+1}}, \tag{4.1}$$

where $B_i = E_n(Ar_i)$ is based on Erlang-B formula.

The rejection ratio, which could be also referred to as call congestion, can be calculated from the formula 3.6.

Equations 4.1 and 3.6 express the preemption probability and rejection ratio for a single rate traffic, where the preemption is removing the lowest priority job from the system. Preemption algorithms discussed in the following sections have different criteria for choosing the flows to be preempted and multi/variable rate traffic is considered. Analytical approach in this case is quite cumbersome, therefore simulations are carried out and algorithms assessment is based on analysis of their results.

4.4 UPnP preemption study

Preemption is one of the QoS mechanisms available in the UPnP-QoS Architecture [55]. As described in Section 3.2, upon failure of the resource reservation procedure, in UPnP's parameterized QoS setup, QoS Manager (QM) can re-attempt the reservation's admittance. This takes place only if the Control Point (CP) requestes usage of the preemption functionality. If this is the case, the QM will request a list of blocking flows' traffic policies, and based on that, it will decide which resources to release. UPnP-QoS defines the QM's release command that passes the *Traffic Handle* parameter while calling Release Admitted Qos action [60]. The protocol does not specify the method for releasing multiple flows. A case of multiple flows release requires multiple Release Admitted Qos

messages to be sent. The specification also leaves to the implementers the design of the procedure that determines what should be preempted and under what circumstances. Below some preemption algorithms that could be used by QM to select the reservations to be released are presented.

4.4.1 Proposed algorithms

In this section, three lightweight preemption algorithms and the motivation for their use are described. The main goal is to propose algorithms with low complexity, which should ease the design and implementation of home network management units like Home Gateways (HGs), set-top boxes etc. Obtained results should show whether using simple algorithms provides acceptable results when: (a) existing reservation preemption and (b) new reservation rejection rates are considered for particular traffic priorities.

Below a description of proposed algorithms is given, followed by the pseudo-code representation of preemption procedure.

1) First-Fit is the simplest algorithm that aims at the identification of a single flow, whose preemption could allow an acceptance of a newly arriving flow. During the search of a particular flow, QM searches through the *ExtendedQoSState* (a message received from a QoS Device (QD) upon reservation failure) and once the candidate flow is identified the search is stopped. The flow that could be a candidate for preemption is the flow that consumes sufficient resources and has priority lower than the new flow requesting the QoS. Afterwards the release action of the selected candidate flow can be performed. If none of the existing reservations comply with both conditions, the preemption can not take place. The pseudo-code of the algorithm is presented below.

2) Minimal Single Fit algorithm looks for a single flow, whose release frees enough resources to allow a setup of a new flow. The reservation selected for preemption has to have lower priority than incoming reservation and at the same time, it should have the minimum priority among the existing reservations. The managing unit searches the whole *ExtendedQoSState* message to identify the single flow that could be subjected to preemption. Similarly to *First Fit*, preemption is not possible if there is no single flow, which satisfies both the priority and resources amount

Algorithm 1 First Fit - Algorithm

```
1: new_prio {New flow's priority}
2: new_bw {New flow' s bandwidth}
3: list ← class_state
4: i ← 0
5: repeat
6:    i ← i + 1
7:    if prio(list(i)) < new_prio&bw(list(i)) + free_bw ≤ new_bw
      then
8:       found ← true
9:    else
10:      found ← false
11:   end if
12: until ((found = true)||(i = size_of(list)))
13: if found = true then
14:   preempt(list(i))
15: else
16:   NOP {Nothing to preempt}
17: end if
```

conditions. The implementation of the algorithm is presented below.

The advantage of previously presented algorithms is the computational complexity of $O(n)$, where n is the number of reservations present in the system. An obvious disadvantage of described earlier algorithms is that they only look for a single flow reservation that consumes resources required for a newly arriving request. It can often be a case that no single flow consumes enough resources that could be released for the higher priority reservation. However, in this situation there could be a *group* of lower priority reservations that consist of flows that together use required amount of resources. This case requires multiple preemption messages to be sent to a single device (due to described earlier, single-flow-release message in UPnP-QoS). Though this procedure takes more time, it can be beneficial in regards to preemption and rejection rates. For this reason the third algorithm is introduced.

3) Minimal Group Fit algorithm is looking for a group of flows. All the reservations in this group should be of a lower importance compared

Algorithm 2 Minimal Single Fit - Algorithm

```
1: new_prio {New flow's priority}
2: new_bw {New flow's bandwidth}
3: list ← class_state
4: i ← 0
5: min_prio ← new_prio
6: repeat
7:    i ← i + 1
8:    if ((prio(list(i)) < min_prio)&(bw(list(i)) + free_bw ≤
      new_bw)) then
9:       found ← true
10:      min_prio ← prio(list(i))
11:      candidate ← list(i)
12:   else
13:      found ← false
14:   end if
15: until i = size_of(list)
16: if found = true then
17:   preempt(candidate)
18: else
19:   NOP {Nothing to preempt}
20: end if
```

to the new reservation, and the sum of the resources that they occupy, once released, should allow a new reservation to be successfully performed. The algorithm defined here takes flow's priority as the major deciding factor. The procedure progresses as follows: minimal priority flow is determined and its resources are added to free resources, if that does not give sufficient resources a second minimal priority flow is identified, its resources are added to free resources variable. Procedure continues until enough resources are freed. The algorithm considers only flows with priority lower than the new request's priority and before hand verifies if the procedure described earlier can be completed. Assuming that the devices can return unsegregated wrt. priority list of current reservations the complexity of proposed algorithm is $O(n^2)$. The implementation of the algorithm is presented below.

Algorithm 3 Minimal Group Fit - Algorithm

```
1: new_prio {New flow's priority}
2: new_bw {New flow's bandwidth}
3: list ← class_state
4: for i ← 1; i < size_of(list); i ← i + 1 do
5:    if prio(list(i)) < new_prio then
6:       candidate_list ← candidate_list ∪ list(i)
7:    end if
8: end for
9: if enough resources in the list then
10:   i ← 0
11:   repeat
12:      j ← 0
13:      min_prio ← new_prio
14:      repeat
15:         j ← j + 1
16:         if (prio(candidate_list(j)) < min_prio) then
17:            min_prio ← prio(candidate_list(j))
18:            candicate_pos ← j
19:         end if
20:      until i = size_of(list)
21:      pree_list ← pree_list ∪ candidate_list(j)
22:      candidate_list ← candidate_list \ candidate_list(j)
23:   until freedenough
24:   preempt(candidate)
25: else
26:   NOP {Nothing to preempt}
27: end if
```

4.4.2 UPnP-QoS preemption model

The model developed for simulations of the UPnP-QoS Architecture and preemption is analogous to the one presented in Fig. 3.1. The CP service implemented, generates the reservation requests in random exponentially distributed intervals, with random uniformly distributed priority and resources amount. The QoS Policy Holder (QPH) manages the policies and returns the requested policy or the list of policies to the requesting QM.

The list of policies is returned for the request containing multiple *Traffic Handles* in a single policy request (typically used during preemption where there are multiple candidates for release i.e., a group of blocking flows). For the purpose of the simulations three QDs of identical structure were used. Each of these devices manages its resources, represented as ten classes of different priorities. Once a request for a new reservation arrives, the QD verifies if it is possible to accommodate this reservation, in the same fashion as described in chapter 3.

If the device's state allows admittance of the new flow, the data of the flow (ID and resources) are added to proper class state and QM is notified about the successfully admitted request. If it is impossible for the device to accommodate the new traffic it will send the fail notification to the QM. In these circumstances, QM will proceed with preemption. First the QM retrieves the *Extended QoS State* of the devices that reservation failed on. The *Extended QoS State* message in our implementation contains information of all ten classes together with flow IDs and the resources they occupy. Later QM makes the decision if there is anything that could be preempted in order to make a new reservation possible.

4.5 Preemption simulation results

In this section the results of the performed simulations are presented. During the simulations a number of characteristics and measurements were obtained. The performance of different algorithms is evaluated based on: the reservation rejection rates in different classes, the preemption rates for different classes, the exceeding resources preemption, and the average class reservation level.

Fig. 4.1, 4.2 and 4.3 show the rejection rate (measured as the number of rejected notifications for a particular priority over the total number of rejection notifications received) for different preemption algorithms. The simulation results clearly show that all the algorithms provide expected rejection fairness for different classes. The improvement in the rejection ratio of new reservations that are requested by CP is relatively low, especially for the middle priority reservations. Obviously, the algorithms that choose minimal priority flows (*Minimal Single Fit, Minimal Group Fit*) for preemption have higher preemption ratios for these reservations. On the other hand, these algorithms are much better at protecting the

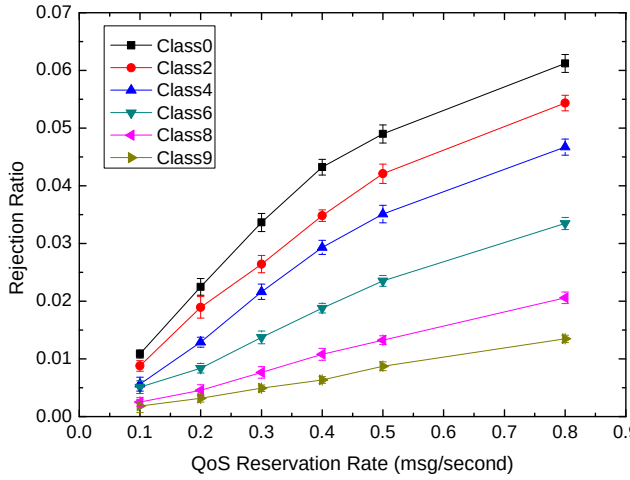


Figure 4.1: Rejection ratio for different priority flows as a function of the flow initiation rate for First Fit preemption algorithm

highest priority reservations, for which the improvement rate is very noticeable, reaching the factor of hundred for the highest priority.

To expose more clearly the differences between the rejection rates for different algorithms, Fig. 4.4 depicts how the rejection ratio differs with changing reservation generation rate for three chosen classes. This graph depicts the fact that protection of the high priority reservations is mainly achieved by higher rejection ratio for lower priority classes, but for *Minimal Group Fit* also the fact that group preemptions are possible plays a role. The numerical data are presented in Table 4.1. One can notice that the *Minimal Group Fit* algorithm rejects very few higher priority requests - the difference between the other two algorithms is less significant.

Additionally, Fig. 4.5 shows how for the proposed algorithms the rejection rates differ with changing priority, for chosen reservation message generation rates (0.3, 0.5, and 0.8 msg/second). This graph shows that priority class five is the reverse point of the rejection ratios for reservation messages generation rate equal to 0.5 msg/second. That means that for *Minimal Single Fit* and *Minimal Group Fit*, comparing to *First Fit*, reservations from classes 6 to 9 are better protected, while reservations from classes 0 to 4 will be more often subjected to rejections. For the

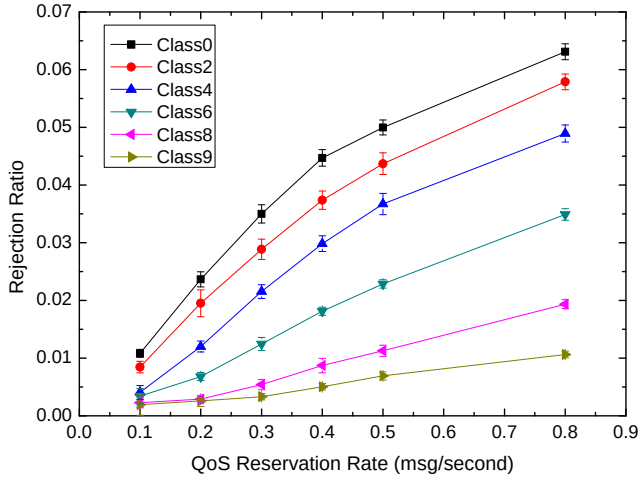


Figure 4.2: Rejection ratio for different priority flows as a function of the flow initiation rate for Minimal Single Fit preemption algorithm

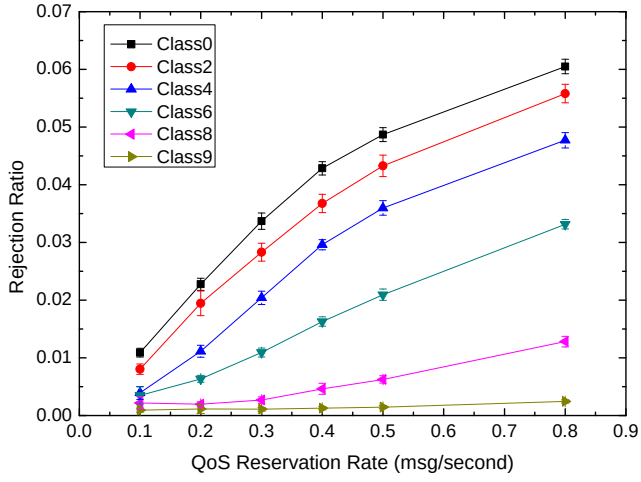


Figure 4.3: Rejection ratio for different priority flows as a function of the flow initiation rate for Minimal Group Fit preemption algorithm

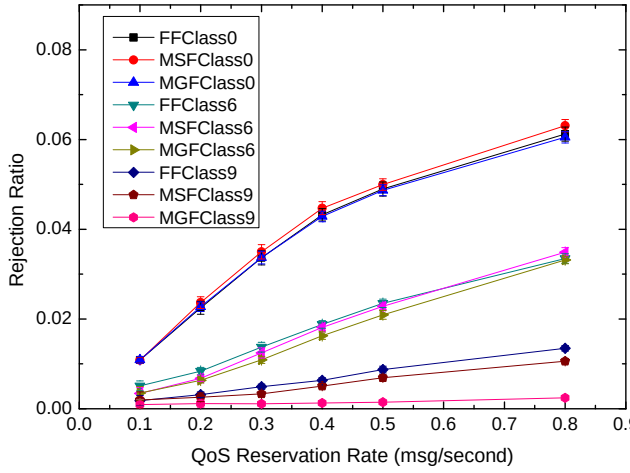


Figure 4.4: Rejection ratio for different preemption algorithms and chosen priorities as a function of the flow reservation generation rate. *First-Fit* - (FF), Minimal Single Fit - (MSF), Minimal Group Fit - (MGF)

Table 4.1: Rejection ratio percentage in particular priority classes for request generation rate 0.5 msg/second

Flow Priority	First Fit Rejection ratio	Minimal Single Fit Rejection ratio	Minimal Group Fit Rejection ratio
0	0.0489	0.0499	0.0487
2	0.0421	0.0436	0.0432
4	0.0351	0.0367	0.0359
6	0.0235	0.0228	0.0209
8	0.0132	0.0112	0.0062
9	0.0087	0.0069	0.0014

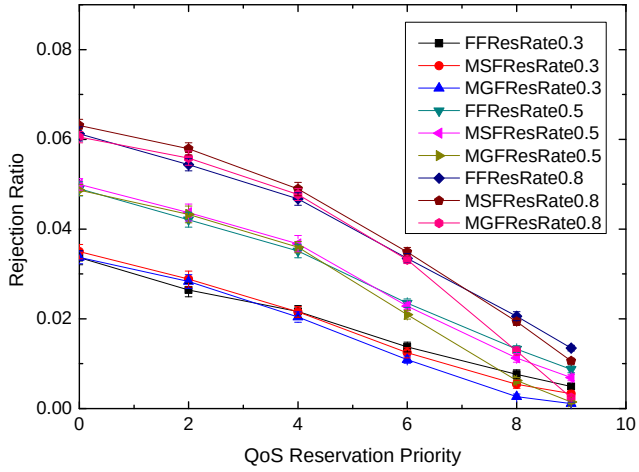


Figure 4.5: Rejection ratio for different preemption algorithms as a function of the flow priority for reservation generation rates 0.3, 0.5, and 0.8 msg/second

reservation request rates 0.3 and 0.8 (msg/second) the reverse points are moved in direction of respectively lower and higher priorities. That is caused by the fact that for higher QoS request rates there is a higher probability of many high priority flows occupying the resources (since these flows will be less often preempted) in the time of a new reservation arrival.

The results of the preemption study show the amount of reservations preempted in particular classes (note: preemption in the highest class is possible as there are multiple priority levels within the class - depending on the flow ID). Fig. 4.6, 4.7 and 4.8 present the preemption of reservations within different classes for the three proposed algorithms. It is clearly visible that the *First Fit* (Fig. 4.6) algorithm does not create the same degree of separation between preemption levels for different classes. This differentiation is more visible for the*Minimal Single Fit* and *Minimal Group Fit* algorithms (Fig. 4.7 and 4.8). Additionally, the *Minimal Group Fit* algorithm lowers the preemption of the highest priority flows even more than the *Minimal Single Fit* algorithm. Fig. 4.9 depicts how for the proposed algorithms, the preemption rates changes with flow priority (data are obtained for reservation message generation rate - 0.5 msg/second).

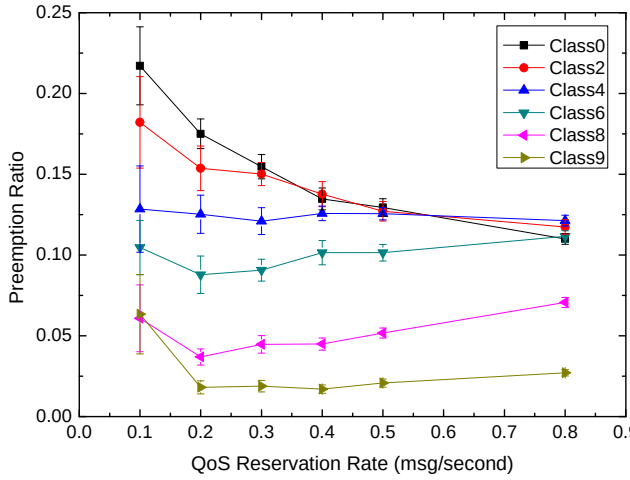


Figure 4.6: Preemption ratio for different priority flows as a function of the flow reservation rate for First Fit preemption algorithm

Table 4.2: Preemption rate percentage within particular priority classes for request generation rate 0.5 msg/second

Flow Priority	First Fit Preemption Ratio	Minimal Single Fit Preemption Ratio	Minimal Group Fit Preemption Ratio
0	0.1294	0.1472	0.1309
2	0.1271	0.1389	0.1293
4	0.1256	0.1276	0.1319
6	0.1014	0.0945	0.1049
8	0.0571	0.0361	0.0404
9	0.0207	0.0029	0.0096

Table 4.2 shows preemption numerical data (fraction of preemptions in a particular class) for different classes and algorithms (data captured for QoS Reservation Rate - 0.5 msg/second).

Fig. 4.10 shows the comparison of the algorithms considering the amount of exceeding bandwidth (BW) that is released during the preemption. The graph shows that both *Minimal Single Fit* and *Minimal Group Fit* are outperformed by *First Fit* algorithm. The difference between the exceeding bandwidth released using described algorithms grows with a growing reservation rate. All algorithms perform better

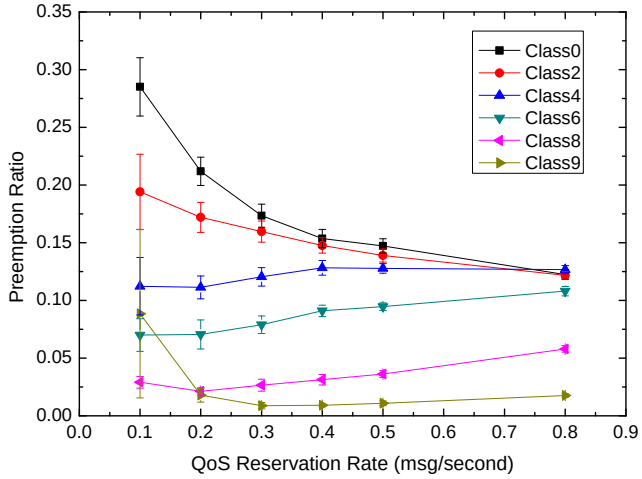


Figure 4.7: Preemption ratio for different priority flows as a function of the flow reservation rate for Minimal Single Fit preemption algorithm

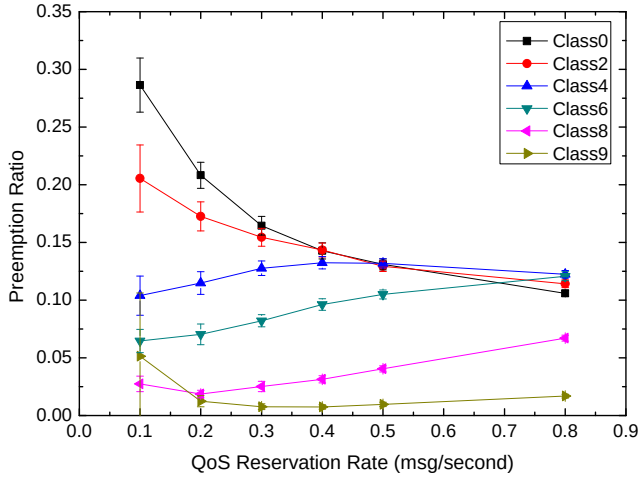


Figure 4.8: Preemption ratio for different priority flows as a function of the flow reservation rate for Minimal Group Fit preemption algorithm

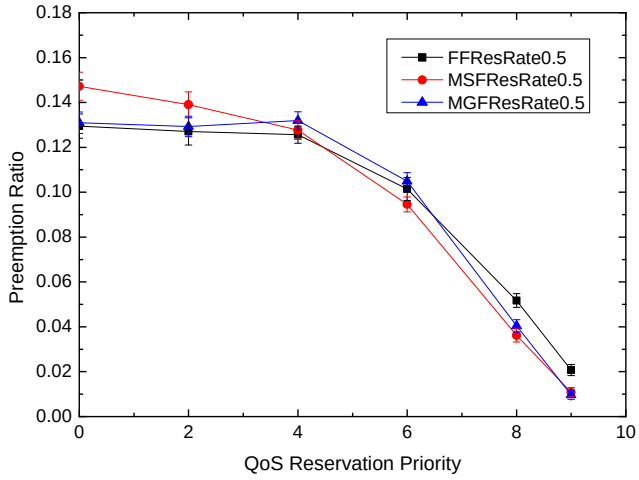


Figure 4.9: Preemption ratio for different preemption algorithms as a function of the flow priority for reservation rate 0.5 msg/second

in regards to exceeding bandwidth release with a growing reservation message rate, which can be explained by a higher probability of small reservations being stored in the devices.

Another performance assessment parameter analysed is the utilization obtained using the different algorithms. Fig. 4.11 shows that all the algorithms archive a similar class occupancy level. This means that on the average the same bandwidth is accommodated on devices' interfaces for all the algorithms. The *Minimal Single Fit* and *Minimal Group Fit* algorithms simply allow more high priority traffic instead of lower priority flows. Though, as showed before, *First Fit* releases less exceeding bandwidth, the resources reserved are on the same level for all three algorithms. That actually means that the other two algorithms readmit flows to utilize the excessive bandwidth of the preempted flows. Whether the exceeding bandwidth preemption is more important than bandwidth utilisation will much depend on the type of traffic in preempted flows, and time/signalling overhead required for its re-admittance. For an interactive traffic (which is probably more likely to be forwarded via *reserved* resources) the preemption would probably mean disruption of the service or drop of Mean Opinion Score (MOS) [71]. On the other hand, for typical data traffic utilisation might be of more importance - as for

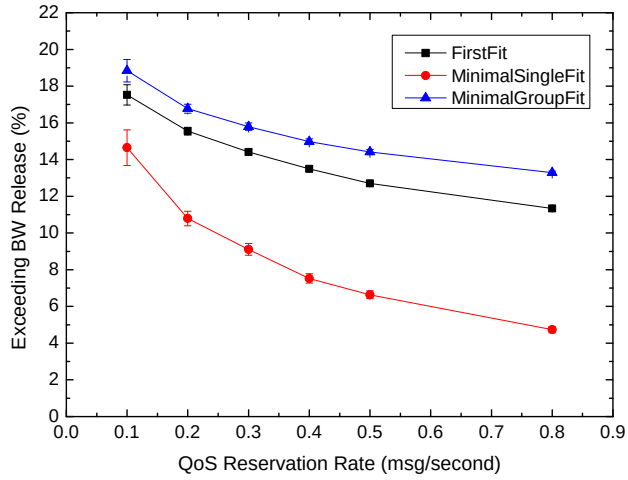


Figure 4.10: Exceeding bandwidth released for different algorithms

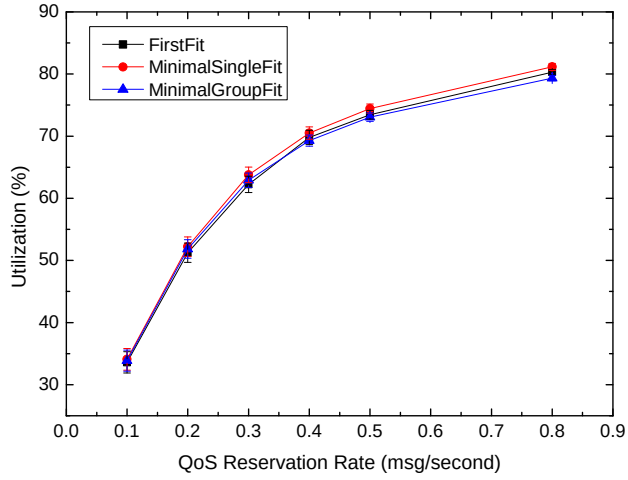


Figure 4.11: Utilization for different algorithms

typical data flows continuous traffic flow is not crucial.

Additionally, as an idea to optimize the preemption procedure, an algorithm that is a combination of *Minimal Single Fit* and *Minimal Group Fit* was tested. This algorithm can switch between the two described preemption methods, identifying a single or a group of flows for preemp-

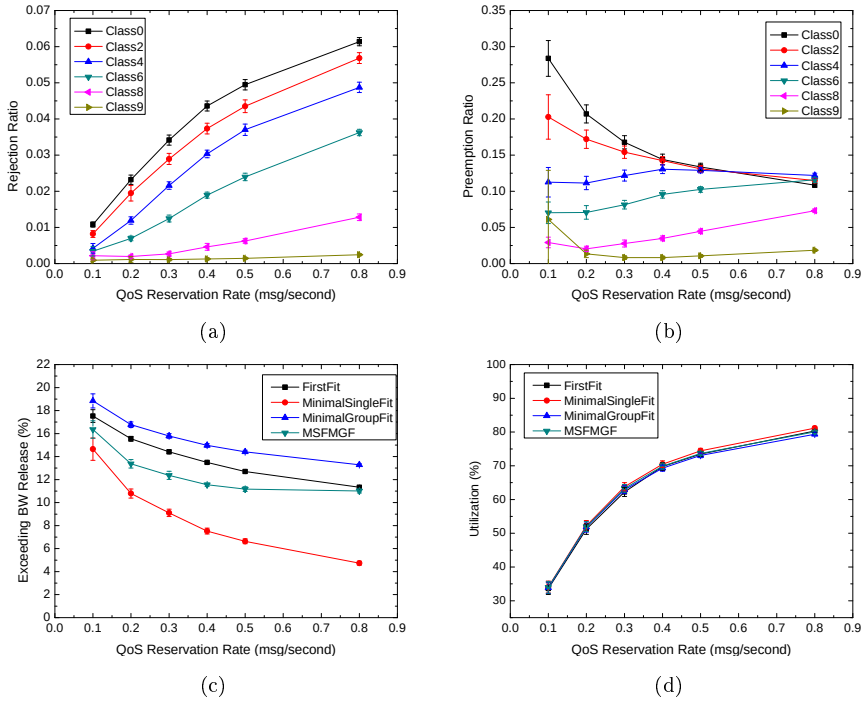


Figure 4.12: Rejection ratio - (a), preemption - (b), Exceeding bandwidth released- (c) 4, and Utilization - (d), as a function of the flow generation rate for the combined MSF-MGF preemption algorithm

tion. The switching between preemption methods could be a method to adapt to changing conditions or requests' priorities. One could use average reservation size, utilisation, or a new flow priority as a decision points for choosing between *Minimal Single Fit* and *Minimal Group Fit* (also other "mix" of algorithms could be considered). As an example, Fig. 4.12 presents an algorithm that uses *Minimal Single Fit* and *Minimal Group Fit* depending on flows' priority. Since computational complexity of *Minimal Group Fit* is higher, it has been reserved for highest priories i.e., priority 8 and 9.

It can be noticed that the combined algorithm exhibits properties of both *Minimal Single Fit* and *Minimal Group Fit* algorithms. While lower classes for both rejection and preemption ratios are identical to results for *Minimal Single Fit*, the high priority classes get the premium

QoS given by *Minimal Group Fit*. At the same time, the computational complexity for average preemption lowers. When exceeding bandwidth released is discussed, the algorithm has an average performance in comparison to those described earlier, which is an expected result for uniformly distributed flow priority. The utilization of the resources remains unaffected.

4.6 NBCP

The previous chapter and sections assumed that devices in the home environment discussed, were compliant with the control and management suite implemented in the home network. To some degree this limits the type of devices and applications that can be part of such network. Especially, when legacy devices are considered, their upgrade to meet control and management requirements might be cumbersome or impossible. It might be also the case that a particular software does not support any functionality that could interface with the QoS management system. Depending on how much traffic these devices and applications can account for, their presence in the network can compromise the QoS established using Control and Managemet (CM) protocol. Using automatic system for traffic classification would lift this inconvenience and allow for more prompt deployment of QoS architectures without the need for total hardware and software update.

The automation of QoS establishment was previously addressed in the context of traffic classification and gateway design. Automatic traffic classification for QoS provisioning was presented e.g., in [72], where a traffic signature based approach is proposed for Class of Service (CoS) marking. In [73] the authors stress the importance of scalability and trade-offs between precision and computational complexity comparing different approaches to automated classification. The scalability is also being addressed by authors of [74], who consider classification in the ISP network, though problems like asymmetric routing and real-time matching vs. ISP network size arise. This section describes the proposal to perform the traffic auto-classification in the customer home network. This addresses the scalability issue and enables flexible in-home QoS provisioning. The following sections present how some UPnP extensions can considerably limit the QoS degradation for scenarios where automatic traffic classification is used to support UPnP-QoS functionality. The work presented here (similarly to the previous chapter) could also be adapted for other service oriented QoS provisioning architectures.

4.6.1 UPnP QoS Architecture - issues

For a case where all the devices are UPnP-QoS aware and all the applications request the resources before they start the communication, the

situation is fully controlled by the QM and the QoS can in principle be preserved for all the flows. We will present the results proving this in section 4.9. Basically, UPnP-QoS Architecture depends on this full control of the network. The specification [55] does not define the actions that should be taken in case the network contains non-compliant with UPnP-QoS devices.

One can consider a number of approaches to deal with the problem of non-UPnP-QoS Devices (devices and applications not compliant with the UPnP-QoS that do not request the resources prior to sending the traffic). The first approach would be to simply discard all the traffic from unknown sources. The second would be granting some limited resources for all the undefined flows and allow them to communicate using only this part of the link. The third approach would be to classify considered traffic and try to create the Traffic Specification for that flow and request proper QoS. Obviously, taking no action can compromise the QoS level for all the network flows. All of the described approaches require some changes to the QoS architecture. They all rely on detection of some traffic properties. In the case of the two first approaches the classification might be fairly simple, while for the third case a more precise classification needs to be performed (e.g., for applications that "hide" under well known ports or perform dynamic port negotiation, etc.). Besides the traffic classifier, there is a need for global knowledge of the established flows. Otherwise it is impossible to distinguish between UPnP and non-UPnP flows. That change could make some of the originally stateless components stateful, while keeping major services stateless is one of the key assumptions for the UPnP-QoS Architecture design, this change should be carefully considered. The following sections, describes the applicability of modern flow classifications for the use in a UPnP-QoS enabled home network, it also contains a proposal of some UPnP-QoS extensions and evaluation of their usability in future home networks.

4.7 Flow classification techniques

Flow classification of today's Internet traffic cannot be based on simple methods using well known port numbers, as these methods were proved to be inaccurate [75]. This is due to a big number of applications using dynamic port negotiation and a growing number of applications trying

to avoid well known ports, or sending their traffic as HTTP flows [76]. These facts lead to a considerable research efforts developing methods capable of flow classification even for a traffic that was designed to pass firewalls and network administrators' filters (e.g., P2P applications and Skype). These methods differ depending on the goal, ranging from long term network planning, security enforcing, and finally QoS provisioning.

In the following sections, the usage of the Appmon application [77] for described use case and architecture is considered. The application uses a three-level classification. The first level uses a packet inspection that checks the payload to identify characteristic application messages. The second level relies on protocol decoding and uses publicly documented application level protocols. Finally, the third layer is based on header inspection. The sequence of the classification levels is aiming at the lowest misclassification possible [77].

Due to protocol control-messages being placed at the beginning of the traffic flow, packet inspection in the described application can usually perform the classification after 100 bytes of the packet payload. This together with 90 percent classification accuracy (describing that nine out of ten flows are correctly classified) creates a good base for flow categorization methods that can be used in network supporting UPnP-QoS provisioning.

Though packet inspection can require high computing power, based on the Appmon's CPU usage [77], it can be said that this (or similar) classification method can be used in the home or office environment in foreseeable future.

4.8 UPnP-QoS Architecture with automatic flow detection

A home network environment with full UPnP-QoS Architecture functionality, together with non-UPnP devices is discussed. To consider any applicability of UPnP-QoS it is assumed that the intermediate nodes (nodes that alone are not sources nor destinations of the traffic e.g., switches, gateways) are UPnP-QoS devices. Otherwise provisioning QoS in a network which infrastructure is UPnP-QoS agnostic would be hardly possible. It also seems more probable for the user to consider the upgrade of a gateway and a switch (maybe few) than all the end-devices in order

to enable QoS. Let us consider for example the network architecture that is presented in Fig. 4.13, where an intermediate UPnP-QoS Device (QD), which will be referred to as Home Gateway (HG) is connected to the remaining UPnP-QoS services namely, QoS Manager (QM) and QoS Policy Holder (QPH) (these services could be also integrated in a typical HG). The intermediate device is also connected to four other QDs. Three of these are running UPnP-QoS compliant sources (requesting the resources before they start sending traffic), and one is a non-compliant device that simply starts sending packets without prior signalling. In a case where some non-UPnP Devices are transmitting, there are a couple of approaches, as described before, to treat their traffic. A solution where home network tries to classify the traffic and support its QoS is chosen. The choice of this option is motivated by the fact that the other two options discussed (discarding and tunnelling) also require modification to the end-devices, providing only a fraction of the functionality of the third approach.

The authors of [78] presened the idea of Automatic QoS Control in UPnP networks by defining a special component i.e., automatic Control Point (CP). This CP should detect the flow in its initial phase and request the QoS from the QM. The authors in their paper focus more on the classification part alone, not considering specifics of interactions between UPnP-QoS Architecture services nor showing how the presence of a classifier influences the QoS level in the network. In the following sections some unresolved issues will be addressed and modifications that allow integration of non-UPnP-QoS devices in UPnP-QoS Architecture will be presented.

One of the unaddressed issues of the approach proposed in [78] is the ability of preventing the end-device from transmitting. Part of the normal interaction between the QM and the CP, as depicted in Fig. 3.2, is the QM reporting an outcome of a resource reservation attempt. In case the QM reports a failure, the CP that usually would be UPnP-QoS aware application, should back-off and try to request resources at a later time. When a centralized Automatic Control Point (ACP) is considered, even in a case of very fast flow classification, where the ACP requests the QoS and receives a failure notification there is no mechanism that can stop the source device from transmitting the traffic and compromising the QoS.

In such circumstances the only way to stop the undesired traffic from malicious devices is to discard it on the first intermediate device so it does not create congestions in the rest of the network. In order to develop this functionality, some modifications to the devices' functionality are needed (at least in the devices being a part of the network infrastructure). A list of UPnP-QoS services, together with required for auto-classification modifications in devices hosting these services, is presented below. The intention is to minimize the scope of these modifications particularly focusing on the stateless character of UPnP-QoS services.

QoS Policy Holder - no modifications are required, remains stateless, identical with standard UPnP-QoS implementation.

QoS Manager - no modifications are required, remains stateless and identical with standard UPnP-QoS implementation.

QoS Device - this UPnP-QoS service does not require the modification itself. The only minimal modification that is required in devices implementing the QD service is the packet marking. All the packets should be marked to indicate packets from UPnP-QoS compliant device (the device remains stateless). This is an optional modification in order to lower the load on the traffic classifier. *QoS Device* service for intermediate devices also stay essentially unmodified, but additionally the intermediate device should be equipped with Network Based Control Point (NBCP). The NBCP is a component that based on the flows classification, requests the QoS from the QM. The packets belonging to flows that were successfully classified and admitted on the path, should be marked as compliant, lowering the load on other classifiers that could reside in the other network components. What makes this approach different from ACP, is that in the proposed architecture the functionality of the CP together with the detector should be placed in all intermediate QDs that interconnect the end devices. In this way network flooding by a non-compliant traffic can be avoided. Additionally, the packet marking is proposed in order to lower the processing power required for the classifiers (it is assumed that at least some traffic will be generated by the UPnP-QoS aware applications and this traffic does not require inspection). Described service should maintain soft state of classified flows,

reset after flow's activity is discontinued (each intermediate device only manages flows originating from directly connected end devices, which lifts scalability issues). The NBCP together with QD functionality would create a new type of the home network device.

This approach allows unmodified QPH, QM and QD with minimal optional change, which results with a possibility of integrating non-compliant devices and applications into UPnP-QoS Architecture.

4.8.1 Model details

Developed model consists of the elements presented in Fig. 4.13. In this case the UPnP-QoS intelligence (QM, QPH) resides outside the switching device. However, one can also consider integration of these components. Each of the presented QDs is equipped with: a) a module managing and reporting the state of its resources according to UPnP-QoS specification, b) a source that generates traffic, and c) a sink used for obtaining statistics. The flows are generated on the CP request with a tunable exponentially distributed rate. The priority of each flow is assigned uniformly between 0 and 7. The resources assigned to flows range between 5 and 40 percent of sub-queue capacity. The pair of source and destination is randomly selected.

The non-UPnP-QoS Device generates traffic in eight classes towards random destinations. The average traffic generated by the non-UPnP-QoS Device is equal to 68 Mbps which accounts for 97 percent of the total amount of resources available on its link. The intermediate UPnP QD has the same UPnP-QoS functionality as the network end devices, with the difference that it is not a source nor destination of any other than the management traffic. It performs switching of packets between the source and destination, and on the outbound interface it queues the packets according to their class. The outbound interface is UPnP-QoS managed by the bookkeeping of interface resources, which means once a request for a new reservation arrives, the QD verifies if it is possible to accommodate this reservation.

The traffic detection is simulated with out-of-band communication between the centralized CP and the non-UPnP-QoS Device. In this way, one can simulate any detection accuracy with high precision. User Importance Number (UIN) of the flows that are detected by the automatic

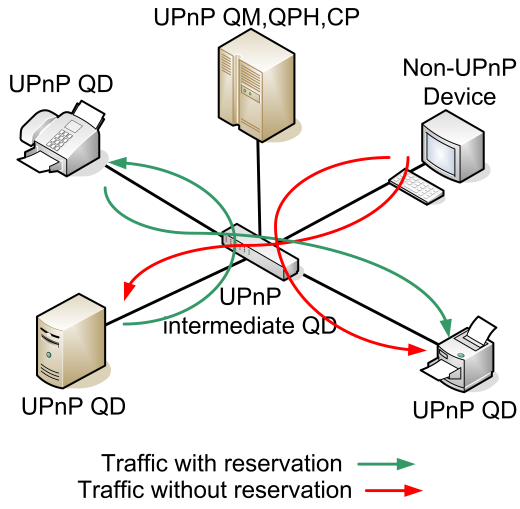


Figure 4.13: UPnP QoS home network model

traffic classification are of the lowest importance in order to allow easier preemption of such flows. The links are considered to be 70 Mbps full-duplex links. Eight classes on the Traffic Importance Number (TIN) level are considered - Class 0 for the lowest priority traffic and Class 7 for the highest. The end devices use FIFO queue for outbound traffic. The intermediate device uses Weighted Round Robin, providing highest bandwidth to classes 7 and 6 (4 x minimum allocation) and lowest to classes 0 and 1 (1 x minimum allocation). The holding time for each of the flows is set to average 15 seconds and the packet delay is measured for the QoS request rate between 2 and 15 requests per second. This gives a range of offered traffic between 30 and 230 percent of the network capacity.

4.9 NBCP - simulations and results

The analysis of efficient traffic classification and its influence on the QoS level in the UPnP-QoS network are based on a number of test scenarios described in this section. First a network fully controlled by UPnP-QoS Architecture is considered. Then, the influence of placing a non-UPnP

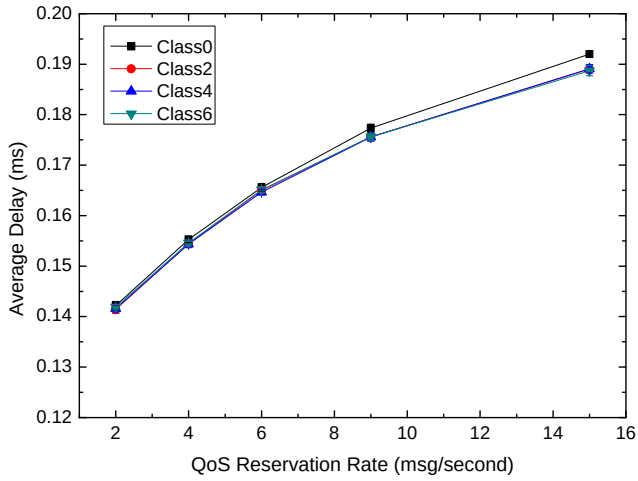


Figure 4.14: Average end-to-end delay for different packet generation rates for full UPnP control

Device in the modelled network is presented. This is followed by improvement in the QoS level after deployment of proposed UPnP-QoS extensions for different traffic classification accuracies. The QoS level is presented by delay and packet loss characteristics as in the model described these are the parameters that will be mainly influenced by the injection of the traffic from non-complaint devices. The chosen reservation rate range allows assessment of network under highly loaded and unloaded conditions.

Fig. 4.14 depicts the results for a fully controlled UPnP-QoS network. It is noticeable that for such a case the delay is limited to a value close to transmission delay ($2 \cdot 512B/70Mbps = 0.12ms$) as the UPnP-QoS functionality, basing on the QDs state reported during QoS establishment, does not allow admission of excessive amount of flows.

On the contrary, Fig. 4.15 presents the QoS level degradation for a scenario including devices non-compliant with UPnP-QoS Architecture. The graph shows the average delay for a situation where a single non-UPnP-QoS device entity generates a number of flows with different priorities. The average bandwidth generated by the non-UPnP Devices, as stated earlier, is 68 Mbps. This 68 Mbps jamming traffic introduces a visible increase of the average packet delay. It is extremely visible

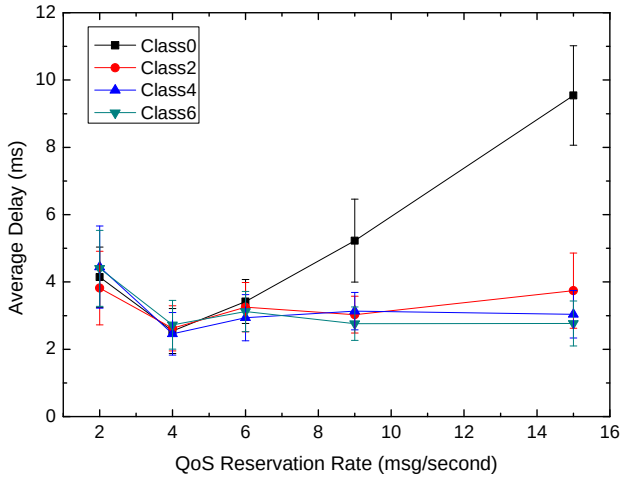


Figure 4.15: Average end-to-end delay for different packet generation rates with UPnP non-compliant devices in the network

for very low priorities, which due to limited resources, are the first to experience bandwidth starvation.

Fig. 4.16(a) to 4.16(d) show the delay results obtained for different classification accuracies (Clf) in different traffic classes. Fig. 4.16(a) shows the packet delay in class 0 for five different levels of classification accuracy. It is noticeable that the lack of automatic QoS requests causes a rapid delay growth, also for 50 percent classification the delay grows fairly fast with a growing QoS reservation rate. For average (70%) and high (90 and 95%) accuracy of classification the delay growth is limited, showing that it can be used as a tool limiting the degradation of the QoS level induced by the non-compliant with UPnP-QoS devices.

Similar conclusions can be drawn from Fig. 4.16(b), which presents the delays in class 2. The figure clearly shows that increasing accuracy for classifier limits the delay.

Fig. 4.16(c) and Fig. 4.16(d) show the delay in class 4 and class 6 traffic respectively. Even though for these classes the growth of the delay is not visible for the investigated QoS reservation generation rate interval (due to highest bandwidth granted by scheduler), one can notice that an increase of classification accuracy significantly lowers the packet delay.

The initial decrease in the delay values visible on the graphs for

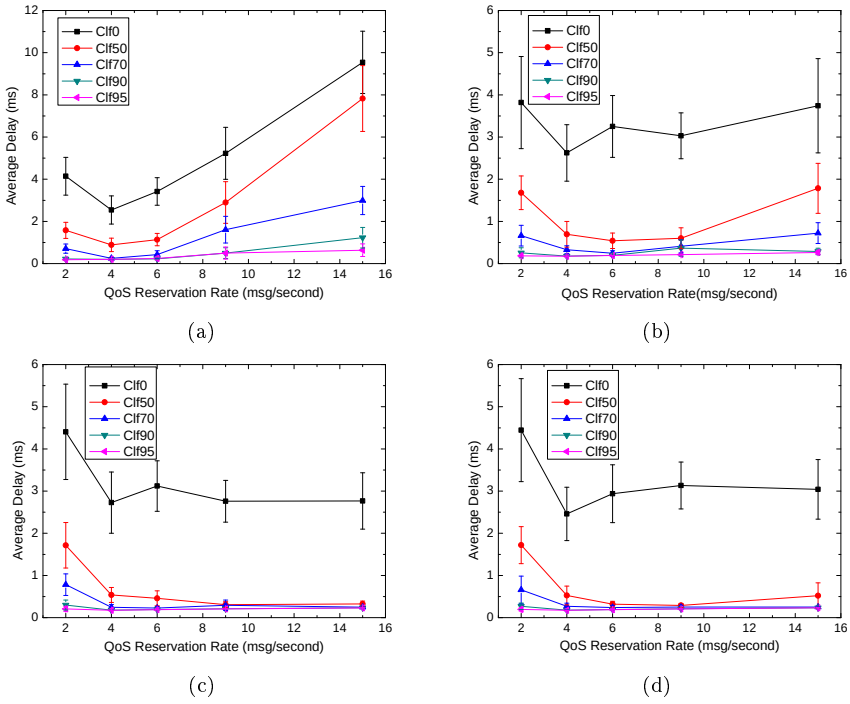


Figure 4.16: Average end-to-end delay for different packet generation rates and detection accuracy for traffic priority (a) 0, (b) 2, (c) 4, and (d) 6

classes from 2 to 6 and low classifications accuracies is caused by the growing share of UPnP-QoS compliant traffic compared to the total traffic volume. Since the average delay is calculated for a traffic originating from both: UPnP-QoS and non-UPnP-QoS devices, and the non-UPnP-QoS traffic rate is fixed, the growth of the UPnP-QoS traffic can cause a small decrease of the average delay values. For higher priorities this tendency is visible for a bigger range of QoS requests due to scheduler properties.

The beneficial influence of the traffic classification is also visible for packet loss characteristics. Since the classification allows traffic policing, it is expected that packet loss will decrease with growing classification accuracy. Fig. 4.17 presents the packet loss for two chosen traffic priorities: (a) for class 0 and (b) for class 6. For class 0 the improvement is clearly visible - where the packet loss value is decreased from 3% to around 1%

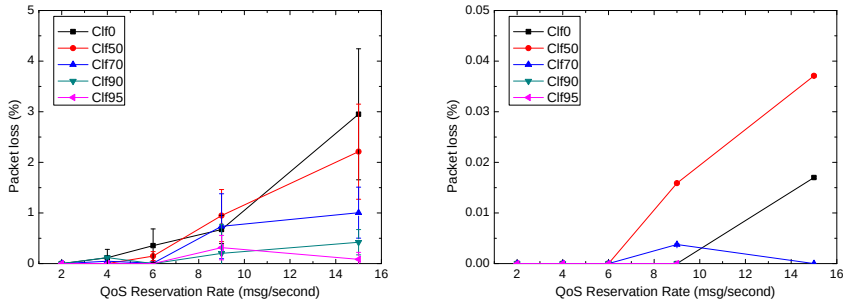


Figure 4.17: Packet loss for different packet generation rates and detection accuracy for traffic priority (a) 0 and (b) 6.

for 70% classification accuracy. For high priority class the packet loss is quite low for all classifier accuracies. For such low packet loss value, the benefits from low classifier accuracy (i.e., 50%) are not really visible. It could be concluded that the improvement due to classifier is mainly concerning classes with higher bandwidth starvation probability.

The comparison of delay measurements for all the flows (those from UPnP-QoS and non-UPnP-QoS devices) presents the improvement obtained by the use of: a) the classifier and b) the UPnP-QoS pre-emption functionality (obviously the latter would not be possible without the classifier). If delay for packets sent only by the UPnP-QoS devices (e.g., for class 2 presented in Fig. 4.18) are considered, one can see that a significant delay value improvement can be also obtained for high classification accuracy, but the average accuracy does not really excel the lack of classification. It can be concluded that low efficiency of traffic classification can be insufficient to increase the QoS level for a compliant traffic, but combined with the proper UPnP-QoS policing (i.e., using UIN in a way ensuring the higher pre-emption probability for non-UPnP-QoS flows) it can be still useful to improve the overall QoS. Finally, high accuracy classifiers bring significant improvement to the delay characteristics for all the cases.

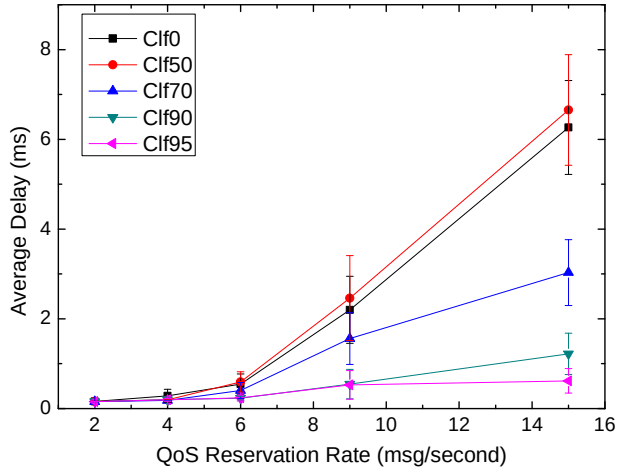


Figure 4.18: Average end-to-end delay for different packet generation rates and detection accuracy for traffic priority 2 - UPnP traffic only

4.9.1 Increased traffic burstiness

The initial simulations were performed for a relatively smooth traffic, which one can expect from the sources that perform traffic admission control. The device that is UPnP-QoS enabled is this type of traffic source. Flows are granted part of links bandwidth and should obey reservation-contract. This usually is implemented by the use of traffic shaper, which smoothens the traffic. On the contrary, non-compliant sources may transmit more bursty traffic. This traffic exhibits self similar properties. For simulating more bursty traffic, instead of using Poisson processes, a heavy tailed distribution should be used e.g., Pareto [79]. The traffic generated in non-compliant devices is obtained by using ON/OFF model with inter-transmission time following Pareto distribution (see equation 4.2) with $\alpha = 1.5$ and $k = 0$.

$$P(\Delta t) = \begin{cases} \alpha k^{\alpha} \Delta t^{-(\alpha+1)} & \Delta t > k \\ 0 & \Delta t \leq k \end{cases} \tag{4.2}$$

The results of delay measurements for bursty traffic from the non-compliant device are presented in Fig. 4.19. The results clearly show that delay values obtained are higher in comparison to results for Poisson traffic. Nevertheless, the influence of the auto-classification and policing of

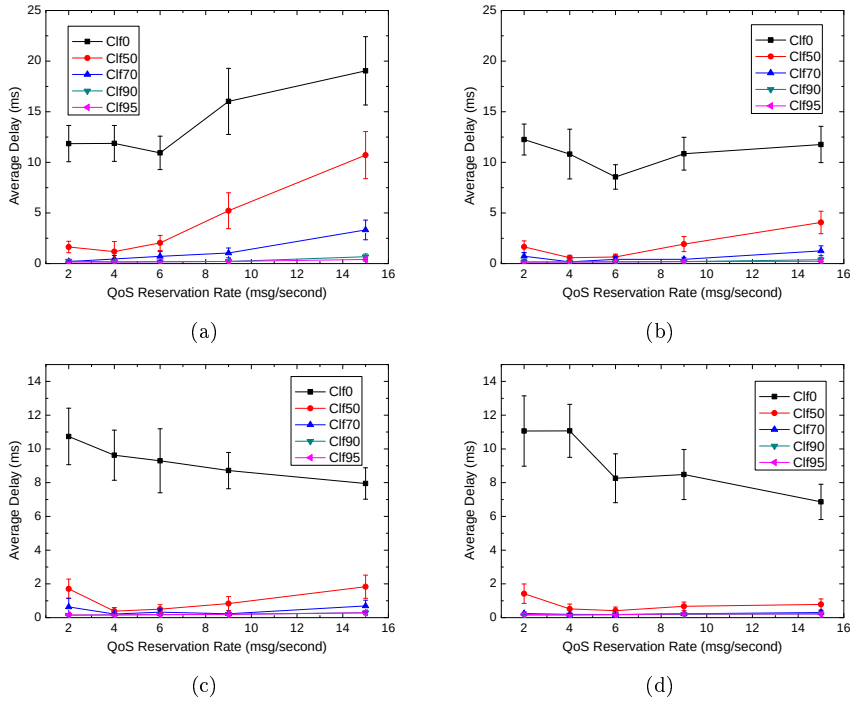


Figure 4.19: Average end-to-end delay for different packet generation rates and detection accuracy for traffic priority (a) 0, (b) 2, (c) 4, and (d) 6

the non-compliant traffic is the same, which validates this QoS assurance technique for more accurately modelled bursty LAN traffic using heavy tailed distributions.

Another worth noticing fact (common for traffic with lower and higher burstiness) is that increasing the classification accuracy makes the delay value much more predictable, which is reflected in smaller confidence intervals. This is an important feature for provisioning QoS for delay sensitive traffic, where admission, path selection, etc., might be dependent on delay value assumptions. Data on the figures are presented with 90 percent confidence intervals.

4.10 Summary

The work presented in this chapter is an extension and completion of UPnP-QoS Architecture. The proposal and performance of three algorithms that can be used for preemption in a home network environment under dynamic conditions have been presented. The results obtained during algorithms analysis show that even the simplest algorithm proposed i.e., *First Fit* provides good fairness of both request rejection and reservation preemption. Additionally, *First Fit* performs better than the other proposed algorithms when exceeding bandwidth release is considered. The results obtained also show that when the highest priority reservations are considered, the *Minimal Single Fit* and *Minimal Group Fit* provide much higher level of protection of the highest priority traffic - where *Minimal Group Fit* performs very well. On the other hand, one has to be aware of higher complexity and possibility of a need for multiple preemptions in order to accommodate single reservation. Due to good performance and only single-flow-preemption the studies here indicate that the *Minimal Single Fit* algorithm can be seen as the most suitable for use in the UPnP-QoS Architecture. Additionally, the advantage of *Minimal Single Fit* over *Minimal Group Fit* is its lower computational complexity.

Finally, the addition to the three proposed algorithms was presented, an algorithm that utilizes *Minimal Single Fit* and *Minimal Group Fit* was analysed. The results show that using flows priority (or other factors) to make a decision upon using one of the algorithms described before seems to be a good solution to obtain satisfactory results for low and average priorities, and give high priority flow the high QoS level. Another benefit from combining the algorithms is lowered average computational complexity.

This chapter also presents the extensions to UPnP-QoS Architecture that allow the coexistence of UPnP and non-UPnP Devices in a single UPnP-QoS based network. By the introduction of the automatic traffic classifiers in the *network devices* that interconnect the end devices, the QoS can be preserved. The model that allows the verification of proposed extensions was presented. It also allows to determine what accuracy of the classifier is required to obtain an acceptable end-to-end delay. The results presented show clearly that for a high ratio of properly classified

flows coming from non-UPnP-QoS devices, the delay values for all TINs can be significantly limited. For high priority classes, the delay values are in fact close to the values obtained for fully UPnP-QoS controlled scenario. It is also important to stress that the modifications proposed do not change the main UPnP-QoS Architecture services nor the interactions between them. They only required modifications concern intermediate devices' functionality, which should allow traffic classification.

Chapter 5

Mapping QoS parameters between home and access networks

This chapter is based on the work presented in [20,24,26–28].

5.1 Introduction

QoS provisioning in home networks, discussed in previous chapters, is a step towards enhancing QoS for the content provided/distributed within home. Nevertheless, still the majority of the traffic that is present in a home environment would cross the boundary between home and access networks. That is why this chapter treats the mapping of QoS aware signalling between the domains discussed. For the home environment, the already described in many details in chapters 3 and 4, Universal Plug and Play - Quality of Service (UPnP-QoS) Architecture is considered. As an access network technology, a packet based Active Optical Network (AON) is discussed. In the scope of AON network the Generalized Multi-Protocol Label Switching (GMPLS) protocol suite is studied, where OSPF-TE and RSVP-TE are considered respectively for, routing and resource reservation. MPLS and GMPLS are often seen as core technologies, however during recent years MPLS usage has been pushed towards the end-customers and is commonly referred to as "MPLS ac-

cess". This together with the common belief that future broadband access should be viewed as the "fourth utility", and the growing need for bandwidth in this part of the network, make GMPLS a good candidate for future control plane.

The flexibility of GMPLS is a motivation for further consideration of this control suite, and investigation of its usability in the Passive Optical Network (PON) area. Including Ten Gigabit Passive Optical Network (XG-PON) under the GMPLS umbrella envisions additional benefits of unified network Control and Managemet (CM), and also is a part of presented QoS parameters' mapping studies.

The remainder of this chapter is organized as follows. The first sections focus on mapping between UPnP-QoS and GMPLS: section 5.2 provides the motivation for home and access QoS integration, section 5.3 treats UPnP-QoS, and section 5.4 describes QoS approaches in GMPLS. These are followed by UPnP/GMPLS mapping strategies in section 5.5. Later the topic of mapping GMPLS and XG-PON is discussed, with motivation for that mapping presented in section 5.6, XG-PON description in section 5.7 and 5.8, and finally the XG-PON/GMPLS mapping described in section 5.9. The summary of this chapter is given in section 5.10.

5.2 UPnP-QoS - GMPLS controlled edge

The use-case that is a motivation for a discussion in the following sections is depicted in Fig. 5.1. The integration of the QoS provisioning in home and access networks allows a preservation of the flow transmission parameters, like delay, jitter and data loss, between the host in the home and server in the access network, e.g., preventing above listed traffic flow parameters from degradation due to background traffic (like in Fig.5.1 the solid line - Video on Demand service being protected from the dashed line - background traffic).

Proposing a control and management plane interface between the UPnP network and GMPLS network is an important step towards the integration of these two important technologies in home and access networks respectively. The integration of QoS within these domains would allow an end-to-end QoS provisioning for services that are provided directly by the access network operator, or services that the operator has

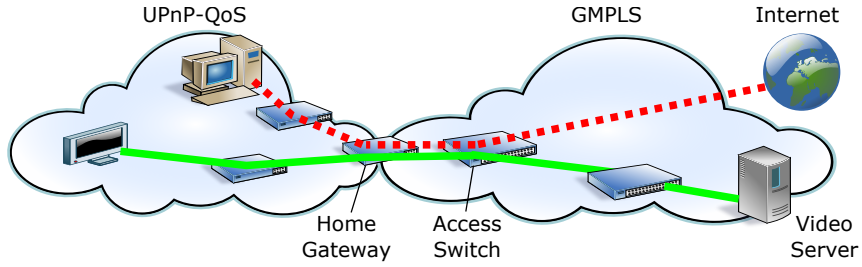


Figure 5.1: UPnP-GMPLS usecase

dedicated connection to, which might be a common case [32, 50].

End-to-end services that traverse more domains, e.g., the entire Internet, are out of scope for this study.

In this chapter the translation of the QoS parameters from one domain to another neighbouring domain will be referred to as mapping, as opposed to the mapping performed between different OSI layers in the same domain (usually in the same network component), which will be referred to as *vertical mapping*.

5.2.1 Related work

Some early work in the field of QoS enabled home gateways is presented in [80], where authors use a QoS-aware Residential Gateway (QRG) for bandwidth management. However, the solution is limited to Differentiated Services Code Point (DSCP) remarking and Class Based Queuing (CBQ) properties adjustment. Also the authors of [81] point out the need for an exchange of QoS information between home and access networks. They propose to outsource the traffic classification to the access network (similar to [74]). They correctly claim that: the use of RSVP requires that applications are specially re-written, per flow reservations raise the scalability issues, and typical consumer equipment potentially lacks the resources for RSVP support. They propose a scheme that requires a copy of user's traffic to be sent to a centralized classifier. The authors of [82] propose a design of IMS-based set-top boxes providing network performance feedback, and allowing the priority increase in the operator's network, similar as [80] the solution is based on DSCP. An investigation of end-to-end QoS establishment and some work on in-

tegration of reservations is presented in [83] where the authors use SIP information to discover the domains to request QoS in. The authors however do not explain how specific QoS parameters (bandwidth, delay, etc.) are signalled in different domains. In [84] the multi-residential gateway is treated, and the Hierarchical Token Bucket (HTB) with First In, First Out (FIFO) queues is proposed for providing link sharing with real-time services. The authors point out that locally managed solutions (like [84] and [80]) are more suitable for QoS support comparing to those that rely on control protocols.

When interaction with the access network is considered in order to provide hard guarantees, traffic marking and shaping alone is usually insufficient and should be combined with signalling protocols. In the following sections, using RSVP for resource reservation is proposed, where reservation itself is HTB reconfiguration (details are presented in Section 5.5.3). When scalability in the access network is considered, in described scenario only a few quality sensitive applications need a translation of UPnP-QoS parameters to access reservations, and scalability is not of a great concern as global end-to-end reservations are segmented into reservations limited to smaller domains. Additionally, 1:1 relationship between application flows and network reservations is not a necessity, i.e., application flows can be merged into a single reservation thus reducing the amount of signalling states.

The work presented here is based on [20] that contributed with the first QoS mapping and signalling schema between a UPnP-QoS based home network and a GMPLS based access network.

5.3 In home QoS - UPnP-QoS

As described in chapter 3, UPnP-QoS defines three types of QoS: prioritized, parameterized, and hybrid. UPnP-QoS uses different parts of the Traffic Descriptor [55] for defining the requirements towards devices' capabilities and configurations. In subsections below the Traffic Descriptor parameters for prioritized and parameterized QoS are presented. Also short summary of UPnP-QoS setup procedures from previous chapters is given in order to put the parameters' description into perspective. Later, section 5.5 discusses the tasks of mapping the parameters conveyed by the Traffic Descriptor to the interface proposed in this thesis, specifying

the input for the establishment of the resource reservations in the access networks.

5.3.1 Prioritized QoS in UPnP

As mentioned previously in this thesis, traffic prioritization usually gives good results in preservation of transmission parameters of different flow types, although only when there is no over-subscription within the priority classes. It is performed by marking packets that belong to different classes with their priority and then treating them differently during forwarding. The main advantage of this approach is its simplicity and scalability, though it is important to point out that a prioritized setup does not provide any end-to-end guarantees since it acts on a per hop basis, and there is no traffic flow specific bandwidth allocation [85]. This type of QoS provisioning is performed by the UPnP-QoS Prioritized setup.

Prioritized QoS setup in UPnP-QoS works as follows: once the Control Point (CP) requested QoS, the QoS Manager (QM) determines which QoS Devices (QDs) should take part in the forwarding of the traffic flow, by invoking the *GetPathInformation* action, it also verifies the state of these devices via the *GetExtendedQosState* action. Next, the QM obtains the Traffic Importance Number (TIN) for particular traffic flow from the QoS Policy Holder (QPH) and attempts the establishment of the QoS on the QDs using the *AdmitTrafficQoS* action, passing the Traffic Descriptor with proper TIN as this action's argument. If no errors occur throughout the above procedure and the configuration of the QDs, the specific traffic flow should be admitted and the QM sends to the CP the UpdatedTrafficDescriptor message containing up to date information about the traffic specification.

As stated before UPnP-QoS does not consider how a QD configures the vertical mapping from TIN to link/network layer prioritization, however the UPnP-QoS specification provides guidelines on how to map the TIN into the VLAN priority tag (802.1Q) and DSCP field, this mapping is presented in Table 5.1. Couple of additional UPnP-QoS/L2 mappings are included in the Interface Addendum [86]. The TIN, besides the TrafficId (used for unique identification of packets belonging to a particular stream), is the only mandatory part of the Traffic Descriptor when setting up prioritized QoS.

Table 5.1: Vertical mapping between UPnP-QoS TIN and link/network layers

Traffic Importance Number	VLAN / IEEE 802.1Q	DSCP priority
0	0	0x00
1	1	0x08
2	2	0x10
3	3	0x18
4	4	0x20
5	5	0x28
6	6	0x30
7	7	0x38

5.3.2 Parameterized QoS in UPnP

In Parameterized QoS, network resources are reserved on all the nodes involved in the traffic forwarding. The reservation is based on a set of parameters such as bandwidth, delay, etc., thus guaranteeing that admitted traffic will be treated in the desired manner. As for the prioritized setup the CP initiates the QoS establishment. Next, the QM requests the topology information from QDs, then policies from the QPH and attempts the traffic admittance on the devices on the traffic path. If the reservation fails the QM can attempt to preempt (if requested) already admitted traffic and re-admit the traffic. Finally, upon successful QoS admittance the QM sends to the CP UpdatedTrafficDescriptor (for parameterized setup containing: rate, end-to-end delay, jitter and other values described later in this section).

The key parameters for setting up Parameterized QoS are placed in the Traffic Descriptor structure, which is passed as an argument of the *AdmitTraffic QoS* action. This will invoke the admission mechanisms towards the network/link layer. Among many parameters included in the Traffic Descriptor the most relevant for the parameterized QoS setup is the *AvaialbleOrderedTspecList*, which contains a list of **Tspec!** (**Tspec!**), the Tspec in turn is composed of a number of traffic parameters. Below the Tspec parameters are listed (precisely the v3TrafficSpecification fragment) together with the unit and indication if the field is; o - optional or m - mandatory, for clarity chosen parameters are shortly described.

- RequestedQosType - o - prioritized, parameterized or hybrid
- DataRate - m - bytes per second
- TimeUnit -o- this integer field specifies the smallest time interval in μs
- PeakDataRate -o- bytes per second
- MaxBurstSize -o- bytes
- MinServiceRate -o- bytes per second
- ReservedServiceRate -o- bytes per second
- MaxPacketSize -o- bytes
- E2EMaxDelayHigh -o- desired upper bound of the End-to-End Delay, in microseconds
- E2EMaxJitter -o- microseconds
- E2EMaxDelayLow -o- expresses that packet delays smaller than E2EMaxDelayLow are not necessary, in microseconds
- QosSegmentSpecificParameters - Interface ID, QoSSegment ID and Segment specific delay and jitter values

5.4 In access QoS - GMPLS/RSVP

GMPLS is a suite of protocols developed by the Internet Engineering Task Force (IETF) for reserving resources in networks that may consist of multiple network technologies, for example Multi-Protocol Label Switching (MPLS) [87], Optical Transport Network (OTN) [88], Synchronous Digital Hierarchy (SDH) [89]. The signalling protocol, RSVP-TE [90], is of interest here as it is responsible for the actual reservations. The GMPLS suite also involves other protocols, e.g., OSPF-TE, [91–93] which is responsible for distributing routing information such as available bandwidth on a particular link (see Fig. 5.2).

RSVP-TE reserves resources by transmitting a request (the RSVP Path message) from the ingress node through the network to the egress

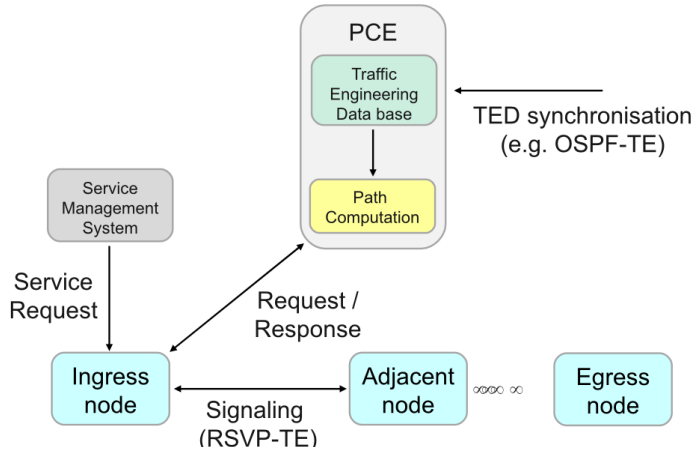


Figure 5.2: The GMPLS architecture

node. The egress node confirms the reservation by replying with a RSVP Resv message which traverses the same path as the request back to the ingress. Any of the network nodes involved in the reservation may upon reception of either message abort the setup by transmitting a PathErr/ResvErr message if e.g., its available resources are less than the requested amount.

A GMPLS network may include other entities separate from the network nodes themselves, such as a Service Management System for initiating the reservation process or a Path Computation Element that calculates which path is suitable for a particular reservation. Since GMPLS is an extensive effort no details of the architecture are presented, more information can be found at the IETF work group CCAMP homepage [94].

5.4.1 Prioritized QoS in GMPLS

Prioritized QoS in GMPLS network is based on the Differentiated Services (DiffServ) where the Per Hop Behavior (PHB) defines how the flows associated with a particular label should be processed in the node, this information is carried in the RSVP-TE DiffServ Object [95]. The RSVP-TE can signal DiffServ for a particular Label Switched Path (LSP) in two ways:

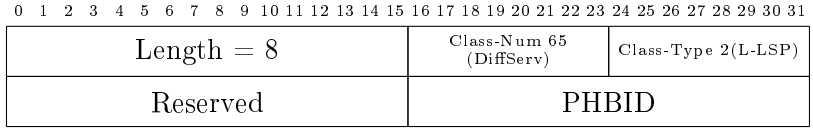


Figure 5.3: DiffServ object for the L-LSP

- For packet oriented networks, E-LSP like approach could be used, where packets or frames can contain priority indication. E-LSP (originally designed for MPLS and named after Experimental (EXP) bits in the Shim header) support multiple Ordered Aggregates (OAs), the priority bits indicate the PHB to be applied to the packet (OAs are the DiffServ Ordered Aggregate, when the traffic belongs to a single OA then it is assigned the same Per Hop Behavior Scheduling Class (PSC) and drop precedence).
- For cases where priority is determined by the label (e.g., for cases where there is no possibility of using the priority bits like in λ switching) L-LSPs are used. L-LSP is used to carry the traffic belonging to a single OA, supports a single PSC that is signalled during the LSP setup procedure (Path message), in this case if Shim is present the priority bits are used for drop precedence indication.

In GMPLS the Shim header in most cases will not be available and consequently it is impossible to pass traffic requirements using the EXP bit. That is why for later described mapping and further implementations L-LSPs are considered. The DiffServ object for L-LSP is presented on Fig. 5.3

5.4.2 Parameterized QoS in GMPLS

In the GMPLS parameterized QoS setup, two types of services are distinguished: Controlled Load [96] and Guaranteed Services [97]. Control Load should provision QoS in order to give a flow forwarding characteristic that a flow would receive in case of unloaded network. The Controlled Load traffic parameters are listed below:

- Token Bucket Rate (r)

- Token Bucket Size (b)
- Peak Data Rate (p)
- Minimum Policed Unit (m)
- Maximum Packet Size (M)

The Guaranteed Services provide a specific QoS with no packet drop guarantees and delay boundaries, and as such the list of its parameters is extended with the delay information:

- Token Bucket Rate (r)
- Token Bucket Size (b)
- Peak Data Rate (p)
- Minimum Policed Unit (m) - used for overhead calculation
- Maximum Packet Size (M)
- Rate (R) - increases the token bucket rate (r) to reduce queuing delays such that - $r \leq R \leq p$
- Slack Term (s) - defines the difference between the desired delay and the delay obtained by using the rate R

The signalling of the QoS requirements in a GMPLS network is handled during the reservation procedure. The RSVP [98] messages Path and Resv contain objects that pass the information of the traffic flow carried in the LSP to the Label Switched Routers (LSRs) on the path. The Path message carries the SenderTSpec object [99] that contains the description of the expected traffic flow. While other objects may change as the message propagates through the network, the Tspec is immutable.

In order to collect the information about the capabilities and resources available on a path, the Path message is carrying the Adspec object that is updated by the traversed nodes. Once the Path message reaches the destination it reflects the end-to-end state of the network path. The Adspec object is composed of a default fragment for both Control Load and Guaranteed Services and from service specific fragments. The default Adspec contains a number of hops, BW estimate,

Minimum path latency, and Composed MTU. If present, the Guaranteed Services fragment contains additional values, rate-dependent (the C term) and rate-independent (the D term) error factors both end-to-end and from the last traffic shaping point.[1]

The Flowspec object is traversing the network in the reverse direction as part of the Resv message and contains the Receiver TSpec that describes the traffic flow and the Rspec defining the desired service parameters required for service to be invoked.

5.5 Inter-domain control and management plane QoS interworking

The studies of the QoS mechanisms and methodologies used in UPnP-QoS and GMPLS show a good match between the UPnP-QoS TrafficDescriptor and RSVP-TE parameters. The following sub-sections will separately treat the mapping for prioritized and parameterized QoS setups.

5.5.1 Inter-domain mapping for Prioritized QoS

In the prioritized QoS setup case the mapping can be considered fairly straight forward. The only parameter that is used in the UPnP domain is the TIN which should be mapped into the PHB in the RSVP-TE domain. For the simplest case, eight TINs could be mapped into the eight different values of the EXP bits, defining one-to-one mapping, though as described before that could be done only for a case of a packet oriented network e.g., MPLS where each packet carries the EXP bit in the Shim header.

For a more general case where the TIN matching has to be done with the L-LSP, the Label Edge Router (LER) connected to the home link has to be aware of what is the level of QoS support in a particular LSP in order to properly match TIN with PHB. It could be realized by having a number of pre-established LSP matching the number of supported classes and the information about the PHBID assigned to a particular LSP stored in the LER. For cases of dynamic L-LSP establishment the

[1] The error term C is the rate-dependent error term. It represents the delay a datagram in the flow might experience due to the rate parameters of the flow e.g., serializing delay; the error term D is a rate-independent error term representing the worst case non-rate-based transit time variation per element [97].

LER needs to ad-hoc match the PHBID with the TIN and setup the LSP with proper PHB properties.

The situation becomes more complex when there is a mismatch in a number of classes in the UPnP home and GMPLS - DiffServ access (that can be a case for example when networks are setup at different times using different policies). For such a case there is a need for class merging or splitting. These could be addressed in a couple of ways:

- The traditional approach would be merging basing on the traffic properties; merging all control and management traffic in one group, all real-time traffic classes in the other group, and similarly with all assured forwarding and all best effort flows.

- The mismatch in a number of traffic priorities could also be addressed in another way. Within the scope of this work also remote management of the Home Gateway (HG) using the TR-069 [100] can be considered. For such a case it would be possible to limit the number of TINs returned by the QPH for flows that would be directed to the access networks, and in this way achieve a one-to-one mapping.

Using TR-069 also addresses, pointed out by [81] the issue of end users responsibility to keep their device's rule sets up to date, since TR-069 would allow to push the responsibility to the Internet Service Provider.

5.5.2 Inter-domain mapping for Parameterized QoS setup

In order to perform a mapping for a parameterized QoS setup (and it is assumed here that both home and access networks support this QoS type) the most important task is to match all required RSVP SendersTSPEC parameters with the UPnP Traffic Descriptor. The part of the Traffic Descriptor that contains the information required for parameterized QoS setup and mapping is the v3TrafficSpecification described in Section 5.3. This UPnP-QoS traffic flow specification has to be mapped into the Control Load or Guaranteed Services parameters described in the previous section. Table 5.2 presents the proposed mapping between

Table 5.2: Mapping between UPnP-QoS parameters and GMPLS-RSVP

UPnP QoS parameter	**GMPLS/RSVP-TE parameter**
RequestedQosType	DiffServ/IntServ
Data Rate	Token Bucket Rate (r)
Time Unit	1000000
Peak Data Rate	Peak Data Rate (p)
MaxBurstSize	Token Bucket Size (b)
MinServiceRate	-
ReservedServiceRate	R
MaxPacketSize	Maximum Packet Size (M)
-	Minimum Policed Unit (m)
E2EMaxDelayHigh	to be calculated - Ctot, Dtot
E2EMaxJitter	to be calculated - Min and Max Latency
E2EMaxDelayLow	Minimum Path Latency
-	Slack Term
ServiceType	0 (CL) or 1 (GS)

the UPnP-QoS parameters and GMPLS/RSVP-TE parameters. Explanation for unmapped parameters and clarification of chosen mappings is described below.

The MinServiceRate parameter is defined as the minimal bit-rate acceptable as a resource reservation for the requesting application [60], it is not mapped as there is no equivalent parameter in the GMPLS domain. This is not considered to be an issue, as the reservation is performed to provision the proper QoS for the service in question and the Data Rate parameter is sufficient for that purpose.

There is no parameter defined in the UPnP-QoS that could convey the Minimum Policed Unit (m) which indicates the minimum size of the processed packets in order to estimate the worst case overhead for bandwidth calculation [99]. The translation of this information is not mandatory though its lack might cause miscalculation of available bandwidth.

Rate R is the reserved service rate, this is the rate parameter contained in the Receivers Specification (RSpec) and reflects the actual rate that is reserved. This information should also be fed to the CP to update the TrafficDescriptor.

Slack Term [97] expressed in microseconds is used to indicate the difference between the requested and obtained delay due to the fact that the packets are transmitted with the Rate R from the RSpec instead of Token Bucket rate r. There is no equivalent parameter in the UPnP domain. However, since this parameter is utilized by the network component to reduce its resource reservation for a particular flow taking advantage from positive Slack Term received from other devices on the path, it is not crucial for QoS level alone. It is rather used for improvement in network resources utilisation, its lack does not compromise presented mapping scheme.

The delay and jitter parameters could be used for path selection, however this is out of scope for this work, instead there is a focus on communicating the delay and jitter values between access and home networks. The most critical delay related parameter is E2EMaxDelayHigh. As the LSR does not have any knowledge about the committed delay in the home network it cannot be sure that the LSP total delay is low enough to meet the requirement of the requesting application.

In order to save resources a LER behavior is proposed where the LSP is released or an error is signaled once the LSP delay is higher than the requested E2EMaxDelayHigh. Additionally, the interface between home and access network should include the possibility of reporting the MaxCommittedDelay parameter (in UPnP-QoS terminology) for the LSP. That will allow the QM to send the E2EMaxCommittedDelayHigh in the UpdatedTrafficDescriptor (being the result of traffic admittance on network devices) to the CP. The UpdatedTrafficDescriptor received by a CP would include delay calculated until the end of the LSP in the access network, which allows the CP to verify if the obtained delay value is within acceptable bounds.

The maximum delay for LSP can be calculated based on the token bucket parameters, C_{tot}, and D_{tot} values according to the formula 5.1 [99]. The resulting parameter, as described earlier, should be mapped to MaxCommitedDelayHigh and should be reported to the QM.

$$max_{E2Edelay} = b/R + C_{tot}/R + D_{tot}, \tag{5.1}$$

where b is the token bucket depth, R is the reserved rate, C_{tot} and D_{tot} are the described earlier error rates.

For reporting MaxCommitedJitter (where MaxJitter is the upper

bound on the end-to-end jitter defined as a difference between the maximum of End-to-End Delay and the minimum of End-to-End Delay [60]) it is proposed that the maximum LSP jitter is calculated based on the Minimum Path Latency (part of the default Adspec [99]) assuming that formula 5.2 holds.

$$\begin{aligned} &MaxCommitedJitter = \\ &\quad max(Jitter_1, Jitter_2, ...) \leq \\ &\quad b/R + C_{tot}/R + D_{tot} - MinimumPathLatency, \end{aligned} \tag{5.2}$$

where $Jitter_n$ is a jitter value based on a number of consequential packet delay measurements.

This value similarly as for the delay values should be reported to the QM which composes E2EMaxCommitedJitter value to be sent to the CP in the UpdatedTrafficDescriptor. The parameters required for delay and jitter signalling would be best conveyed by returning the Adspec to its source i.e., the sender.

5.5.3 Implementation

In order to verify the usability of proposed solution the gateway function, called the Adapter was developed. The implemented interface is based on OSGi framework and acts as an intermediate between the home and access networks. Upon receiving a QoS request the module converts the UPnP Traffic Descriptor into parameters expected by the access network testbed. The access network used is based on a number of virtual machines running a modified version of the GMPLS suite DRAGON [101] controlling a Linux user-space implementation of 802.1Q, 802.1ad, 802.1ah, 802.1Qay data plane. The Adapter connects to the DRAGON module and based on the Traffic Descriptor determines the end points of the LSP. The IP addresses that corresponds to these end-points are used by DRAGON for actual LSP creation. Later the Adapter processes the received Traffic Specification and priority parameters and passes this information to be used in LSP creation through the use of the RSVP protocol message exchange between involved LSRs along the LSP.

Beside the LSP establishment a couple of additional issues needed to be addressed. Namely, the routing of the traffic to proper LSPs and

installation of Traffic Control (TC) rules on the testbed nodes.

For the purpose of aforementioned functionality two scripts were developed, this also required the Adapter to poll the DRAGON process for upstream and downstream LSP labels in order to provide mapping information to the scripts. The first script, which associates client and server traffic with the proper LSP, is running on the edges of the LSP and the Adapter is triggering its actions passing the upstream and downstream label respectively for far and near end of LSP (seen from the Adapter point of view). This script creates the interface, routing and ARP table entries required for routing of the newly admitted traffic to the proper LSP. The second developed script is used for enforcing QoS rules on the data flow that is forwarded through the user space Ethernet switches. This is done based on the Traffic Specification parameters from the Adapter and through the use of the Linux function HTB Queuing Disciplines (qdisc) together with filters matching forwarded packets into the HTB classes created for the admitted traffic flow. The architecture of the testbed is depicted in Fig. 5.4.

5.5.4 Test scenario

The assessment of the QoS provided, correctness of traffic routing and shaping in the network was based on a measurement of data flow parameters in the presence of background traffic. The measurement using IPerf and the evaluation of perceptional quality for video streaming were used. Both methods verified proper establishment of forwarding rules and QoS handling of traffic flows through the home and access edge. The benefits of such interface are straightforward as stated in the motivational part of this chapter. The perceptional quality for video streaming [102] that was used during the tests is presented in Fig. 5.5 - showing the result of streaming before QoS establishment and Fig. 5.6 showing the frame after the QoS was established. In the virtual environment used in the testbed the setup time through all the components along the path (including LSRs and script execution) was around 5 seconds. Though the result is not impressive one could consider it would be sufficient for a case of LSPs established at the time of the service initiation. Additionally, this could be improved with the modification of the RSVP module. It should also be emphasized that the goal of this work is to verify the functional

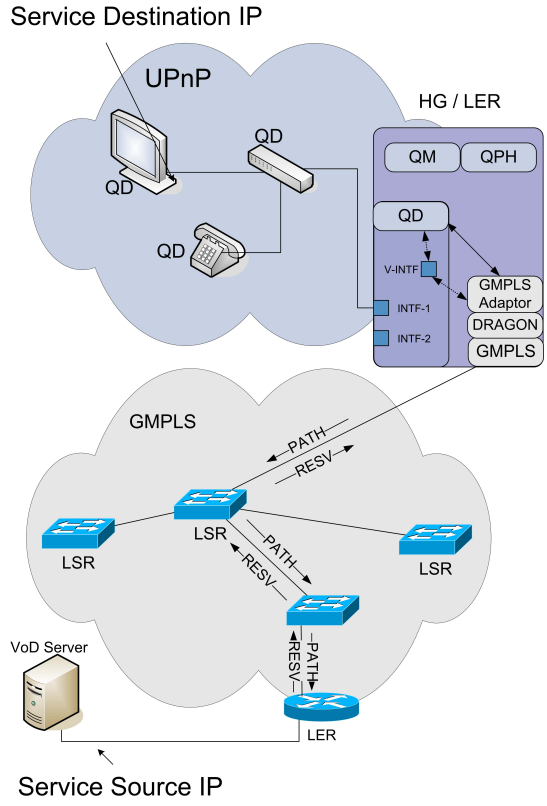


Figure 5.4: The UPnP/GMPLS testbed architecture

Figure 5.5: The frame captured from the video before the QoS establishement

Figure 5.6: The frame captured from the video after the QoS establishement

aspects and not performance aspects (e.g., optimize the setup time).

5.5.5 Network security consideration

When deploying a system that allows an end-user interact with the access network control plane, security is a large concern. It would be advantageous to integrate QoS-setup with existing Authentication, Authorization and Accounting (AAA) [103] solutions, where users are authenticated and granted access to certain services. The amount of accessible resources could be controlled by the users account type and one could imagine that for example premium subscribers would have access to more resources and/or have priority in case of preemption etc.

5.6 GMPLS XG-PON mapping - motivation

Benefits from a uniform control plane of networks in the access/metro and possibly home domains are rather straight forward. To mention some - coherent management tools may simplify the network Operations Administration and Maintenance (OAM), reducing the number of human error related outages in the networks, plus the possibility of resource management automation and in many cases lower operation costs.

Today Passive Optical Networks (PONs) and Active Optical Networks (AONs) technologies compete for an access part of the network. The most popular PON technologies being deployed nowadays are Gigabit PON (GPON) and Ethernet PON (EPON). In general EPON is characterized as the simpler and cheaper technology while GPON is perceived as more flexible but at the same time more complex.

Considering AONs, the main interest is in commonly used control suite i.e., Generalized Multi-Protocol Label Switching (GMPLS) using Resource ReserVation Protocol with Traffic Engineering (RSVP-TE) for reservation of the resources in multi-layered environments.

While using GMPLS for Ethernet control is a subject with several papers published, and test-beds developed, there are no implementations of the GMPLS controlled PON networks. The following sections present the proposal of the integration of the GMPLS control with PON networks. This could enable the end-to-end QoS provisioning assuming GMPLS complaint home edge and metro/core networks. While GMPLS enabled core and metro networks are common, the GMPLS compliant home edge is still rather rare. The latter though aligns with the growing popularity of Digital Living Network Alliance (DLNA)/UPnP products. It was shown in the previous section that the set of parameters used in UPnP-QoS Architecture for enabling QoS in home networks is a good match with GMPLS/RSVP parameters. Presented Home Gateway (HG) functionality that can initiate an Label Switched Path (LSP) setup based on the UPnP request is a good example of GMPLS capable home network edge. Therefore considering GMPLS based core/metro network and GMPLS enabled HG, the control and management of the access part of the network might be a crucial aspect for enabling end-to-end QoS provisioning. Which is the motivation behind the consideration of the benefits of including the PON technologies into the end-to-end GMPLS architec-

ture. XG-PON is particularly interesting as in comparison with GPON and EPON it provides more bandwidth that is more likely to meet future demands. Additionally in comparison to its precursor i.e., GPON, it is also more flexible concerning the traffic management and addressing.

5.6.1 Related Work

There is not much work done in this area, though some attempts to introduce RSVP in EPON can be found in [104]. Unfortunately the authors do not explain the details of mapping and traffic containers matching, they rather assume the fact that GMPLS can be used for EPON management. The authors of [105] propose a new simplified MAC signalling, which we consider unnecessary as it does not offer a solution to the problem of PON management using GMPLS. Also [106] is treating GMPLS controlled EPON. The authors again assume GMPLS compliant Optical Network Unit (ONU) and Optical Line Terminal (OLT) focusing on node mobility for architecture where the Base Stations are fed from the ONU, and a mobile user can move between Base Stations connected to different ONUs and also different OLTs.

5.7 XG-PON basics

XG-PON [107] developed by ITU is an evolution of GPON [108] that should enable a ten-gigabit per second connectivity on the PON networks. Two main nodes can be distinguished in XG-PON: in a central office the OLT and at user premises ONUs. The OLT is connected via a fiber with passive splitter with a number of ONUs, which take turns to communicate with OLT. XG-PON uses fixed size 125 μs XG-PON Transmission Convergence (XGTC) frame for upstream and downstream transmission. OLT's downstream XGTC frames and ONU's upstream XGTC bursts are composed of a number of XG-PON Encapsulation Method (XGEM) Frames that belong to different logical connections, which are identified via associated Port-IDs. The OLT schedules the ONU's upstream access to the shared media in static or dynamic fashion. Dynamic approach besides providing fairness between different ONUs, can also provide more elaborated QoS support.

XG-PON's documentation defines that a service specification (or traffic descriptor) shall be associated with traffic flows mapped to XGEM

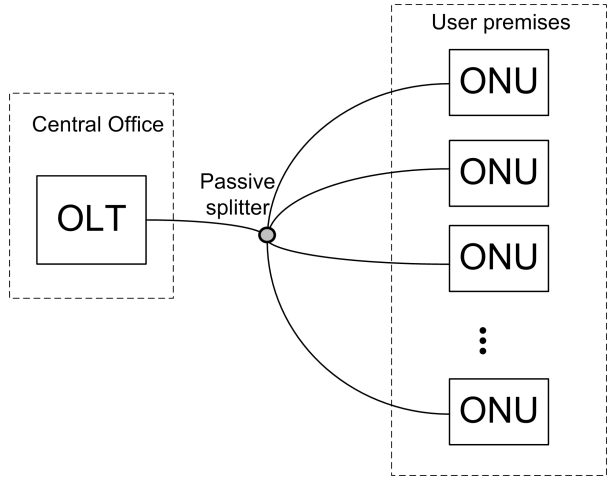


Figure 5.7: The GMPLS architecture

Port-IDs. This service specification is a set of service attributes that characterize the service type, contracted QoS, and flow parameters, which typically include Committed Information Rate (CIR) and Peak Information Rate (PIR). Downstream QoS management is OLT based, where policing, shaping, and queuing is performed on a XGEM port basis. Upstream traffic QoS is managed at two different levels, by OLT on per Transmission Container (T-CONT) basis and by ONU based on association with a particular XGEM Port-IDs.

5.8 Details of OLT/ONU management

This section focuses on the analysis of the available QoS mechanism that can be enabled in XG-PON. Especially important here is Dynamic Bandwidth Allocation (DBA) that due to architecture properties is the most significant QoS tool especially when the upstream traffic is considered. There is also a couple of important matters that seem to be open to implementers' choice which will also be treated in this section as they have major influence on the proposed in this chapter GMPLS managed XG-PON.

5.8.1 Dynamic Bandwidth Assignment and Allocation

According to the XG-PON specification, DBA refers to the distribution of upstream transmission opportunities but the work presented here considers bandwidth distribution in both directions i.e., also specifying the allocation of downstream bandwidth from OLT to the particular ONUs[2]. When the downstream traffic distribution is considered, all the functionality for QoS management is centralized and resides in the OLT. In this point-to-multipoint architecture the OLT has all the knowledge about the traffic that has to be transferred to the ONUs. The amount of bandwidth for upstream traffic port depends on DBA but also on the allocation performed in the ONU. Traffic management in both downstream and upstream directions is depicted in Fig. 5.8 and will be described is sections below (Sections 5.8.3 and 5.8.2).

5.8.2 Downstream traffic

The downstream traffic assignment is done on XGEM Port-ID basis and as XGEM port identifies a single individual logical connection it provides high resolution for resource allocation. The XGEM Port-ID is a 16 bit number and provides 64512 assignable IDs[3]. Assuming split ratios from 1:32 through 1:64 to planned 1:128 this creates a possibility of assigning between 504 and 2016 XGEM Port-IDs per ONU. Even considering the multi-dwelling building scenarios where several apartments are connected to a single ONU the number of XGEM Port-IDs that are available for each user seems to be sufficient for addressing all logical connections (which was not that obvious for GPON, with its limited IDs). Additionally, for multi-dwelling situation it is assumed that 1:32 split ratio is more reasonable to focus on. Higher split ratios, as long as 10 Gbps downstream capacity is considered, would mean rather limited bandwidth per user. This limited throughput could hardly meet future services' requirements.

[2]The term "bandwidth assignment" refers to the distribution of the upstream capacity between the ONUs, while the term "bandwidth allocation" refers to granting individual transmission opportunities i.e., XGEM ports

[3]1022 are implicitly assigned with and is equal to ONU-IDs, one is idle

5.8.3 Upstream traffic

In the upstream direction, based on the service specification of the multiplexed XGEM-Ports, aggregated T-CONT specification is created. T-CONT is an ONU object representing a group of logical connections that appear as a single entity for the purpose of common handling and upstream bandwidth assignment in PON network. Normally, the sum of fixed and assured bandwidth components should be equal to the CIR of constituent flows in a particular T-CONT. Maximum bandwidth should not be smaller than PIR [109]. When the traffic aggregated in form of T-CONT is considered, it is the responsibility of the OLT to provide QoS aware traffic management based on the available resources and traffic monitoring or status reporting information. It is the responsibility of the ONU to provide QoS enabled traffic management of individual traffic flows identified by the XGEM-Port-ID, and based on the specification of the individual traffic flows. Additionally, the ONU upstream traffic management toolset for resource allocation and QoS handling may include: ingress traffic policing, traffic shaping, and XGEM Port-ID flow scheduling, within a T-CONT [109].

T-CONTs

ONU creates a number of T-CONTs, though this concept is introduced only for simplification referring to most commonly used Allocation Identifier (Alloc-ID) traffic descriptors. The T-CONT type is not communicated between ONU and OLT, instead XG-PON handles Alloc-IDs based on the traffic descriptor parameters. The supported T-CONT instances are created during the activation of the ONU (number of these instances is a fixed number for a given ONU). In order to learn about the number of supported T-CONTs by a particular ONU, OLT uses Optical Network Unit Management and Control Channel (OMCC). To carry the traffic associated with a particular T-CONT the OLT must set the Alloc-ID attributes in T-CONT that it wants to activate. The mapping of the Alloc-ID to a particular T-CONT is a one-to-one mapping.

Most vendors support multiple T-CONTs per ONU. In theory the number of T-CONTs is only limited by the possible number of identifiers. No other indication is present in the documentation, however vendors might limit the number of supported T-CONTs due to cost related issues.

As described earlier, the work presented here assumes the split ratio 1:32. In theory since there are 15360 possible Alloc-IDs (Alloc-ID identified traffic-bearing entity can be T-CONT or OMCC, there are 1022 default IDs for each ONU and one broadcast ID) with 1:32 split ratio one can talk about up to 480 T-CONTs per ONU. That makes it possible to consider quite high-granularity of upstream flow grouping, allowing flow per T-CONT assignment in case of specific, high demand flow types. This gives a particularly high flexibility in T-CONT ID assignment for cases where ONU is installed for a single user, which also meets anticipated bandwidth requirement, that are expected to be measured in hundreds of megabits per second. Nevertheless, even if a smaller amount of T-CONTs per ONU is considered, one can still argue for per Alloc-ID LSPs, as long as the number of T-CONTs is sufficient for supporting all different types of services available at a single home network. That means that per XGEM-Port upstream traffic management might not be necessary. Though one needs to consider that as T-CONT is representing the group of connections there will need to be at least one GEM-Port associated with this T-CONT in order to create the traffic flow.

Bandwidth maps

Another concept used for upstream bandwidth assignment is the bandwidth map (BWmap), which is an array of allocation structures, where each of them represents a single allocation for a particular T-CONT. The BWmap data is generated by the OLT and sent to the ONUs. It contains Alloc-ID of the T-CONT that is granted the bandwidth, start-time and stop-time indicating the interval in which the ONU is allowed to transmit.

5.9 GMPLS controlled XG-PON

In the scope of this work the unification of the control plane has its main motivation in need for the end-to-end QoS provisioning. When GMPLS control is considered the most relevant issue for QoS provisioning is the reservation of the resources being part of the LSP establishment. This section presents the proposal of LSP establishment over XG-PON. Based on the background and more detailed information in the previous sec-

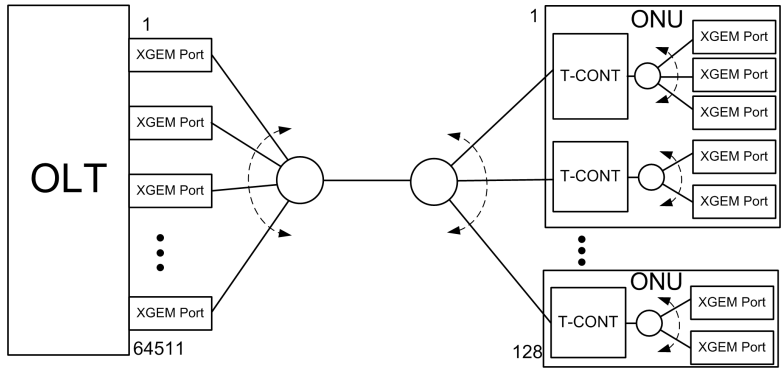


Figure 5.8: XG-PON scheduling

tions, signaling requirements for QoS enabled GMPLS based resource reservation in XG-PON network are presented.

5.9.1 Possible approaches for nodes' management

In GMPLS there might be different levels of control applied to nodes in the network. A specific node can be addressed (e.g., in Explicit Route Object (ERO) for case of path calculation) or a group of nodes can be treated together. These two levels of abstraction are referred to as *simple abstract node* and *abstract node* respectively [110].

OLT and ONU as independent RSVP nodes

This situation is equivalent to OLT and ONU acting as simple abstract nodes. Both ONU and OLT will process the PATH and RESV messages. In this case both devices check available resources and admittance is performed separately. Both the ONU and OLT needs to be GMPLS enabled and should be able to identify the resources and match the received Traffic Specification into proper T-CONT and/or XGEM-Port. Besides that both nodes should update the Adspec. When the label is considered the nodes need to signal which Alloc-ID/GEM-Port-ID tuple will be used to identify a particular flow (more details in section 5.9.2).

XG-PON abstracted into a single node

In principle one could aggregate the PON network into an abstract node. That would allow to communicate the RSVP messages only to OLT and the ONU could be GMPLS unaware. It would be the OLT's responsibility to provide the QoS level that was indicated in the PATH message (if the reservation was accepted). In case the OLT cannot support the requested QoS within the abstract node i.e., within the XG-PON, it should reject the reservation. If the reservation can be admitted the OLT should update the Adspec fragment considering delay and jitter in the entire PON network and send it to the next GMPLS aware node (e.g., Home Gateway connected to the ONU). There is a potential problem when abstracting the network into a single node. Without the knowledge of internal links' state the PCE has no data to ensure that the calculated path is the optimal route to a particular destination and there might be many failing attempts of reservations.

One solution to this issue is the possibility of aggregation of the internal subnet connectivity and represent it through the advertised parameters of an external link. For such a situation the external link is presented as of the capacity:

$$Link_{BW} = min(BW_{ext}; BW_{int_1}; BW_{int_2}; ...BW_{int_2}), \qquad (5.3)$$

where BW_{ext} is the bandwidth in the external (seen from the abstract node) link and BW_{int_n} are the bandwidth values of the possible paths through the nodes creating the abstract node. This might create yet another problem since this information can cause the rejection of the reservation that would normally follow the internal path (path in the abstract node) with $BW > min(BW_{int_1}; BW_{int_2}; ...BW_{int_n})$.

Though an important feature of the PON needs to be considered, its point-to-multipoint topology ensures that all the traffic passes through the OLT. In this topology the external OLT link's state should be up to date and the formula 5.3 is sufficient to provide up to date PON status through advertising the parameters of the external link.

The above means that both simple abstract node and abstract node can be considered for GMPLS management of XG-PON.

5.9.2 Possible approaches for resource allocation

The concept of XGEM-Port and T-CONT allows for two major approaches for binding LSPs with XG-PON traffic containers.

Per T-CONT upstream LSP, per XGEM-Port downstream LSP

It seems that the best option is if the LSP setup will be performed by binding the upstream path with a particular T-CONT and the downstream path with XGEM-Port.

Downstream traffic is only distinguished by the XGEM-Port-ID and as such the XGEM-Port-ID is the only choice for label on the PON network segment. Upon receiving the LSP request the OLT will determine the next hop basing on the ERO or routing information. This should allow for the determination of the ONU-ID and possibly Port-ID to reach the destination (whether that information is preconfigured or learned using dynamic protocol is out of scope of this analysis).

When upstream traffic is considered, it also needs to be associated with the XGEM-Port-ID. However, it does not mean that the XGEM-Port-IDs need to be the labels for established LSPs. It seems beneficial to use the Alloc-ID as part of the label. In particular associating the label only with Alloc-ID might be beneficial. The main reason for that is that if the traffic associated with a single LSP is associated with a single Alloc-ID one can be quite certain about the provided level of QoS, since it is Alloc-ID's descriptor that determined how the upstream traffic is scheduled.

Per XGEM-Port up/downstream LSP

An other approach would be using XGEM-Port-ID as a label for both upstream and downstream traffic. For downstream traffic the situation is the same as in the previous section. For upstream traffic each flow should be associated with XGEM-Port-ID like in the previous section but this time it is assumed that the single Alloc-ID will accommodate a number of ports. These ports would belong to different LSPs. This approach would be required for ONUs with a limited number of Alloc-IDs, which could be a case for high split ratios. On the other hand these

ONUs would need to be equipped with some admission mechanism that would prevent from over-provisioning within the Alloc-ID (not to exceed the capacity of the traffic container defined by its parameters).

5.9.3 Reservation of the resources in the XG-PON network

In this section possible approaches for RSVP processing in the XG-PON network are covered. The reservation procedure is asymmetric and because of that reservations in the OLT and ONU are a bit different (this is assuming that ONU is GMPLS enabled like for the simple abstract node approach).

For both cases it could be considered that the LSP will be associated with a XGEM-port and the upstream GEM-Port will also need to be associated with T-CONT. There are 64512 possible port IDs and that would be a limit of the possible number of LSPs.

For admitting a new LSP i.e., after arrival of a Path message in OLT or ONU the following actions should take place:

- Check bandwidth availability, and proceed if enough resources or send Path Error.
- In OLT assign a new XGEM-port or associate the new flow/LSP with an existing XGEM-port and provide proper queuing according to the service description, using, *Matching technique* (see section below).
- In ONU assign/reuse a XGEM-port, more importantly associate the traffic with a correct T-CONT matching the service description.
- Extract the LSP's BW from an available BW, both at the OLT and in the ONU (ONU deducts capacity from a proper T-CONT).
- Update the Adspec and forward the Path message to the next node, wait for the Resv message to finalize the reservation.

Matching technique

Matching is defined as a procedure of assigning traffic with certain QoS needs described by TSpec to the XGEM-Port and/or TCONT that is

proper for supporting this traffic requirements. Since it is out of scope of the specification how OLT and ONU are scheduling the traffic, a couple of assumptions need to be made. In our opinion it is not invalid to assume that OLT and ONU implement scheduling scheme similar to Hierarchical Token Bucket (HTB)[4]. In such XG-PON device matching between TSpec and XGEM-Port is straight forward. Data rate, peak-rate and bucket size from the TSpec can be mapped respectively to rate, ceil and burst parameters of HTB. In OLT HTB schedules XGEM-Ports carrying different downstream flows, while in ONU separate HTB would be required per each T-CONT (that obviously is a case only for T-CONTs with multiple XGEM-Ports). For every time-slot granted by DBA algorithm to a particular TCONT, its HTB would be allowed to schedule a corresponding number of packets from XGEM-Ports being members of this T-CONT. Admitting XGEM-Port to existing TCONT needs to fulfill R_F^{tot} and R_A^{tot} (total fixed and assured bandwidths components of T-CONT) requirement according to Eq. 5.4 (where R_F^j, R_A^j are fixed and assured bandwidths components of constituent flows within T-CONT). If this can not be fulfilled there is also a possibility of T-CONT update. When updating the T-CONT the capacity (C) requirement needs to be checked (see Eq. 5.5).

$$R_F^{tot} + R_A^{tot} = \sum_j R_F^j + R_A^j. \tag{5.4}$$

$$\sum_j R_F^j + R_A^j \leq C. \tag{5.5}$$

Updating the Adspec

Another relevant procedure that needs to be considered when GMPLS management of XG-PON is described is the Adspec update. Each node that is participating in the reservation needs to update the Adspec that is attached to the Path message. In this way the accommodative state of the devices is presented to the destination and a decision about traffic admission can be made. The list of the parameters that need to be updated during Adspec processing is presented below.

[4] Linux implementation of HTB is well popularized and not difficult to use

- IS hop count - simple incrementation .
- Path BW estimate - update according to the rate of a particular XGEM-Port.
- Minimum path latency - as it is an end-to-end latency in the absence of any queuing delay, it will be dependent on the distance between OLT and ONU, which is known after the ranging procedure.
- Composed MTU - minimum of all the MTUs.
- Ctot, Dtot, Csum, Dsum (for Guaranteed Services Adspec) - these parameters are hard to determine without some knowledge of the DBA algorithm. It has been shown in [111] that delay is very much influenced by the DBA flavor, and as such C and D values should be assessed for specific DBA used.

Buffer status overwriting

One could also utilize DBA and LSP setup at the same time and instead of using only fixed allocations a part of the bandwidth could be used for assured and non-assured traffic. This approach in some cases can allow more flexible bandwidth management. In such scenarios, means of influencing DBA might increase promptness of the bandwidth allocation scheme. In order to manipulate the DBA mechanisms in Status Reporting DBA (SR-DBA) one might need to overwrite the buffer status, which in consequence would force the ONU/T-CONT to be scheduled. Otherwise one can expect the delay required for DBA convergence (see Fig. 5.9 inspired by [112]). For Traffic Monitoring DBA (TM-DBA) the DBA depends on the empty frames being sent, that would mean that the ONU needs to "mislead" the OLT by sending the non-idle traffic, even though it is idle. Before one decides about using this approach it should be understood that it might be seen as non-compliance with the standard, and it can have negative effect on network utilization.

Reporting/updating the TE-link states - OSPF

It is important to keep the neighbor maintenance, flooding and database reservation as efficient as possible. This efficiency in OSPF broadcast

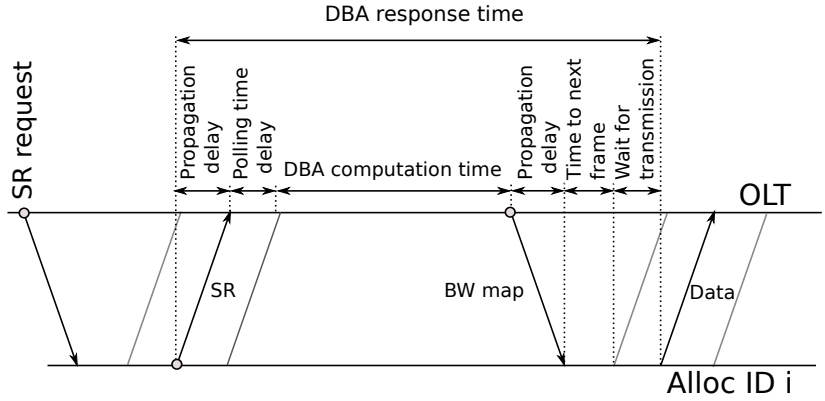


Figure 5.9: PON - DBA

subnets is achieved by selection of the Designated Routers which limits the neighbors pair number from $n{\cdot}(n{-}1)/2$ to n (where n is the number of routers). In Point-to-MutliPoint OSPF Subnets there are not Designated Routers. The Hello protocol detects the active OSPF neighbors and the neighbors simply synchronize the database with all adjacent routers. For topologies close to full-mesh that can lead to $O(n^2)$ maintenance complexity. However, in PON network this will not be the case. Since the OLT interconnect all the ONUs and none of the ONUs are directly interconnected with each-other, there are only n router pairs - as it is for Nonbroadcast Multiaccess (NBMA) segments or broadcast subnets with Designated Routers.

5.10 Summary

This chapter presented a proposal for the integration of the UPnP-QoS architecture in home network with GMPLS based access. The parameters required for inter-domain QoS provisioning were outlined and the mapping between different domains was presented, while making sure that the translation of all relevant information was performed. Presented signaling allows reporting delay and jitter parameters in order to achieve an end-to-end view of those parameters during traffic setup procedure. The work presented here, contributes with a test setup where an interface enabling the integration of UPnP-QoS architecture with GMPLS

test-bed was developed and demonstrated.

In this chapter the possibility of integrating XG-PON with the GMPLS controlled environment was also presented. GPON has currently the highest market share among PON technologies in Europe and North America, with extensive roll-outs planed in China [113]. In consequence, it can be considered a very important technology worldwide, which due to possible upgrades to XG-PON, makes the latter significant future FTTH solution. Therefore the study presented here can provide admonition for future converged and end-to-end QoS enabled home edge, access and metro networks - utilizing a GMPLS based unified control plane.

Chapter 6

Reservation and reduction factor in multi-rate multi-server networks

6.1 Introduction

More and more services provided by data networks have strict QoS requirements. In consequence this caused the development of many QoS techniques with two main, already described in this thesis categories i.e., Differentiated Services and Integrated Services. While the first provides only traffic differentiation, the latter gives more explicit guarantees by dedicating a part of resources on the path to the requesting service. Growing processing power in routers and increasing popularity of GMPLS and RSVP for LSP establishment, make resource reservation more often a choice when the QoS provisioning is considered. At the same time the amount of video traffic is rapidly growing and it is said to be the majority of the Internet traffic soon. This highly compressed video traffic exhibits high ratio between its peak and minimal data rate, i.e., it is said to be very bursty.

Reservation of resources according to the peak data rate provides a high level of QoS but to a large degree lowers links' utilization. Therefore, it would be beneficial to reserve only a certain fraction of the peak rate (closer to the average rate). At the same time it might cause higher

packet delay or even packet loss, which in order not to degrade QoS and the user experience, should stay in a reasonable range.

Reservation of bandwidth in the amount of R, where R is smaller than P (peak data rate) has been covered in [114]. The authors show that choosing the reservation rate below the peak data rate allows admission of more flows. They propose the use of the equivalent bandwidth as a reservation parameter. They define this bandwidth as the bandwidth that allows obtaining a target queue length and loss probability. The analysis presented show that equivalent bandwidth is dependent on the amount of back ground traffic, but also P/L ratio (where L is the link rate).

The authors of [115] address the issue of highly bursty traffic on a different layer. They use hybrid MAC for wireless networks and perform the reservation for a part of the video traffic while allowing the remaining video traffic to compete for the channel during contention periods.

Rate degradation and guaranteed minimum data rate together with maximum data rate was discussed in [116]. The author considers both bufferless and buffered models but deals only with single rate traffic.

Reservation of resources in form of trunk reservation has been studied in [117] and [118] where multi-rate traffic is blocked in case the bandwidth consumed by a particular flow exceeds a certain reservation value. Here, IntServ and RSVP meaning of resources reservation is considered. I.e., a particular traffic flow is guaranteed an access to a dedicated fraction of the link and the traffic exceeding this reservation (in RSVP terminology non-conforming packets) shares the remaining resources with other traffic flows. Usually the packets outside the reserved rate are treated as Best Effort (BE) traffic. This does not necessarily ensure the fairness at the flow level, which could be considered as not optimal.

This chapter presents an analysis of a queuing network with multi-server multi-service traffic with guaranteed minimal amount of resources. A partial reservation is considered, where reserved resources are guaranteeing packet delivery for a part of the traffic flow, while a part of the link's bandwidth is not available for any reservations. instead it is used as a common resource shared between all flows. Additionally, during congestions the reduction factor is defined. It is used in order to carry the bursts of all the flows (without blocking them) by adjusting the service rate. This approach will give a higher fairness between flows as granting

resources in the common capacity is based on the state of the system and reservations for all the services. Additionally, it is worth pointing out another advantage of the approach described here i.e., where sharing of a part of the capacity is considered. For such a case, if equivalent bandwidth is slightly incorrectly calculated one can still utilise statistical multiplexing in order to get fair QoS comparing to hard-boundaries reservations where the non-conforming traffic is dropped or treated on the Best Effort basis.

6.2 Reversible multi-server multi-service nodes

A system similar to [119, 120] or [121] is considered, with n_j servers (or channels) assigned to flow j, plus additional n servers that are shared between all the flows that require more than n_j servers. There are N different traffic streams, λ_j denotes the intensity of arrival process for flow j, and $d_j\mu_j$ describes the service rate.

The state of the system is defined as:

$\underline{x} = \{x_1, x_2, ..., x_j, ..., x_N\}$ where x_j is the number of channels occupied by type j customers, as stream j requires d_j channels per connection the following notation is introduced:

$\underline{x} - d_j = \{x_1, x_2, ..., x_{j-1}, x_j - d_j, x_{j+1}, ..., x_N\}$.

Due to limited resources the reduction factor is calculated, but only for shared capacity. The reduction factor needs to ensure reversibility.

$\overline{x}_j$ is defined as the state of the flow j in the additional/shared capacity, so:

$\overline{x} = \{\overline{x}_1, \overline{x}_2, ..., \overline{x}_{j-1}, \overline{x}_j, \overline{x}_{j+1}, ..., \overline{x}_N\}$.

If the capacity used by the flow is higher than the reserved capacity n_j and the system is overloaded, the service rate is reduced for the packets using the capacity above the reservation amount.

The reduction factor $g_j(\overline{x})$ is calculated as follows:

a) For non feasible states: $x_j \leq 0$

$$g_j(\overline{x}) = 0, \qquad j = 1, 2, ..., N. \tag{6.1}$$

b) For states with flow's j demands smaller than reserved capacity: $0 \leq x_j \leq n_j$

$$g_j(\overline{x}) = 1, \qquad j = 1, 2, ..., N. \tag{6.2}$$

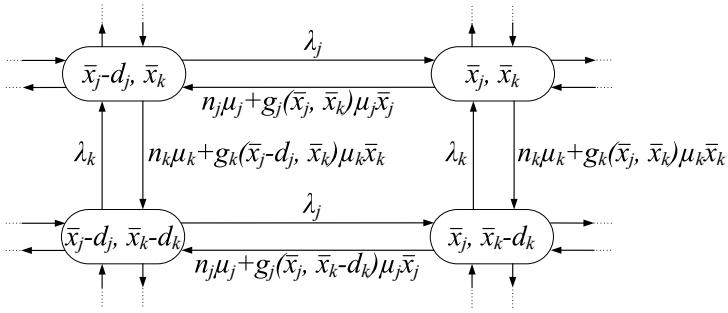


Figure 6.1: State transition diagram for the system with two classes (j, k)

c) For states where some flows exceed their reservations but additional capacity is meeting their demands:

$\{\sum_{j=1}^{N} x_j \leq \sum_{j=1}^{N} n_j + n\}$ and $\{x_j \leq n_j + n \ \ \forall j\}$

$$g_j(\overline{x}) = 1, \qquad j = 1, 2, ..., N. \tag{6.3}$$

d) For states where one type of service has demands higher than available capacity both within its reservation and in the additional capacity: $\{x_j \geq n_j + n\}$ and $\{x_i \leq n_i,\ i \neq j\}$

$$g_j(\overline{x}) = \frac{n}{\overline{x}_j}, \qquad j = 1, 2, ..., N. \tag{6.4}$$

e) For states where multiple types of flows have demands exceeding their reservations and additional capacity: $\sum_{j=1}^{N} x_j > \sum_{j=1}^{N} n_j + n$, we consider four states:

$(x_1, ..., x_j - d_j, x_k, ..., x_N)$ $\qquad$ $(x_1, ..., x_j, x_k, ..., x_N)$

$(x_1, ..., x_j - d_j, x_k - d_k, ..., x_N)$ $\qquad$ $(x_1, ..., x_j, x_k - d_k, ..., x_N)$

Since rate reduction is only considered for traffic above the allocation, one can define:

$\overline{x} - d_j = \{\overline{x}_1, ..., \overline{x}_{j-1}, \overline{x}_j - d_j, \overline{x}_{j+1}, ..., \overline{x}_N\}, \overline{x}_j \geq d_j.$

To maintain reversibility the reduction factors need to fulfil the Kolmogorov cycle condition (see Fig. 6.1):

$$\lambda_k\lambda_j(n_k\mu_k + g_k(\overline{x})\mu_k\overline{x}_k)\cdot(n_j\mu_j + g_j(\overline{x}-d_k)\mu_j\overline{x}_j) = \tag{6.5}$$
$$= \lambda_j\lambda_k(n_j\mu_j + g_j(\overline{x})\mu_j\overline{x}_j)\cdot(n_k\mu_k + g_k(\overline{x}-d_j)\mu_k\overline{x}_k),$$

so

$$g_j(\overline{x}) = \frac{(n_k + g_k(\overline{x})\overline{x}_k)\cdot(n_j + g_j(\overline{x}-d_k)\overline{x}_j)}{(n_k + g_k(\overline{x}-d_j)\overline{x}_k)\overline{x}_j} - \frac{n_j}{\overline{x}_j}. \tag{6.6}$$

Considering normalization equation:

$$n = \sum_{j=1}^{N}\overline{x}_j g_j(\overline{x}) \tag{6.7}$$

$$= \sum_{j=1}^{N}\frac{(n_k + g_k(\overline{x})\overline{x}_k)\cdot(n_j + g_j(\overline{x}-d_k)\overline{x}_j)}{(n_k + g_k(\overline{x}-d_j)\overline{x}_k)} - n_j, \tag{6.8}$$

we finally get:

$$g_k(\overline{x}) = \frac{n + \sum\limits_{j=1}^{N} n_j}{\overline{x}_k\cdot\sum\limits_{j=1}^{N}\frac{n_j + g_j(\overline{x}-d_k)\overline{x}_j}{n_k + g_k(\overline{x}-d_j)\overline{x}_k}} - \frac{n_k}{\overline{x}_k},\ j\neq k. \tag{6.9}$$

6.2.1 Performance evaluation

Once the probabilities of different system states were obtained, different aspects of system performance can be calculated. Below different parameters together with their calculation methods are listed (in the following k refers to the buffer size).

Blocking probability (Pb):

$$Pb_j = \sum_{\underline{x}\in A\cap B} p(\underline{x}), j = 1, 2, ..., N. \tag{6.10}$$

where $A = \{\underline{x}|x_j \geq n_j\}$ and $B = \{\underline{x}|\overline{x} \geq n + k - d_j\}$.

Full-service probability (Ps):

$$Ps_j = \sum_{\underline{x} \in C \cup D} p(\underline{x}), j = 1, 2, ..., N. \tag{6.11}$$

Where $C = \{\underline{x} | x_j < n_j\}$ and $D = \{\underline{x} | \overline{x} < n - d_j\}$.

Delay probability (Pd):

$$Pd_j = \sum_{\underline{x} \in E \cap F} p(\underline{x}), j = 1, 2, ..., N. \tag{6.12}$$

Where $E = \{\underline{x} | x_j \geq n_j\}$ and $F = \{\underline{x} | n - d_j \leq \overline{x} < n + k - d_j\}$.

Mean Queue Length (MQL):

$$L_j = \sum_{\underline{x}} p(\underline{x})(x_j - n_j) \cdot (1 - g_j(\overline{x})), \qquad j = 1, 2, ..., N. \tag{6.13}$$

Carried Traffic:

$$\begin{aligned} Y_j = & \sum_{\underline{x} \in G} x_j \cdot p(\underline{x}) + \\ & \sum_{\underline{x} \in H} \big(n_j \cdot p(\underline{x}) + (x_j - n_j) \cdot p(\underline{x}) \cdot g_j(\overline{x})\big), j = 1, 2, ..., N. \end{aligned} \tag{6.14}$$

Where $G = \{\underline{x} | x_j \leq n_j\}$ and $H = \{\underline{x} | x_j > n_j\}$.

Mean Waiting Time (MWT):

$$W_j = L_j / Y_j, \qquad j = 1, 2, ..., N. \tag{6.15}$$

6.3 Multi-rate multi-service queueing networks

In this section a network composed of the nodes described above is considered.

6.3.1 Open networks

To find state probabilities of an open queueing network is relatively easy. The load in each node for each chain can be calculated from flow balance equation:

$$\Lambda_k = \lambda_k + \sum_{j=1}^{N} \Lambda_j \cdot p_{jk}, \tag{6.16}$$

where λ_k is the intensity of customers/packets arrival to node k from outside, and p_{jk} is the probability of a packet being transferred from node j to node k.

As there is product form between the nodes, calculation of the state probability for the network is given by:

$$p(x_1, x_2, ..., x_K) = \prod_{k=1}^{N} p_k(x_k). \tag{6.17}$$

Where $p(x_1, x_2, ..., x_K)$ describes probability of network being in the state where there x_k customers in the k^{th} node.

6.3.2 Closed networks

First, the relative load in each chain and each node is derived from flow balance equations. Next, the aggregation of nodes by multi-dimensional convolutions, keeping account of the number of customers in each chain, is performed. All nodes except the target node are aggregated to one node, then finally the aggregated node is convolved with the target node, and the performance measures are obtained. The convolution is defined as follows:

$$p_{1,2}(x_1, x_2, ..., x_K) = p_1 * p_2 = \tag{6.18}$$
$$\sum_{i_1=0}^{x_1} \sum_{i_2=0}^{x_2} ... \sum_{i_N=0}^{x_N} p_1(x_1 - i_1, x_2 - i_2, ..., x_N - i_N) p_2(i_1, i_2, ..., i_N).$$

Table 6.1: Parameter of services

Service	Total bandwidth [Mbps]	packet rate [pps]	frame size [kb]
Service 1	1.8	30	60
Service 2	3.6	60	60

6.4 Case study

This section presents three different case studies that utilize the theory presented in the previous sections. The software developed for this purpose is based on the program developed for [122].

6.4.1 Single node

First, a single node with two types of services is considered. One service might be a high priority video for which the reservation is performed, and the second service is e.g., some low priority traffic flow with no dedicated resources. The services can be defined as follows:

Service 1 - the high priority video - sends 30 frames per second and requires on the average 1.8 Mbps.

Service 2 - the background traffic - sends 60 packets per second and consumes on the average 3.6 Mbps.

Table 6.1 summarizes parameters of the services.

Assuming channel size (Basic Bandwidth Unit - BBU) equal to 1.8 Mbps, gives $d_1 = 1$ channel/packet for *service 1* and $d_2 = 2$ channels/packet for *service 2*, and respectively 0.032 and 0.016 seconds mean service times. The offered traffic is assumed to be: for *service 1* equal to 10 erlangs and for *service 2* equal to 15 erlangs. This, based on $A = \frac{\lambda}{\mu s}$, results in $\lambda_1 = 300$ and $\lambda_2 = 1800$ with respectively 10 and 30 channels required for *service 1* and *service 2*.

The total number of channels that is required for two described services is 40 channels. Assuming 80 percent utilization, a node with 50 channels is defined, buffer size is chosen to be $k = 100$. For a node defined, earlier described scheme for resource sharing with guaranteed minimum is applied.

Two resource allocation approaches will be discussed in this section, they are summarized in the Table 6.2. The *n1* parameter describes the

Table 6.2: Channels allocation schemes for single node analysis

Channel allocation scheme	Total number of channels	k	n1	n2	nA
1	50	100	0→16	0	50-n1
2	50	100	6→16	50-n1	0

number of channels dedicated for *service 1*, *n2* is the number of channels dedicated for *service 2*, and *nA* is the number of channels accessible for both services). *Scheme 1* presents an allocation approach where some part of the resources is dedicated to high priority service requiring the protection, while the remaining resources are accessible by all the services. This scheme is referred to as scheme *with sharing* (WS). *Scheme 2* on the contrary is a *no sharing* (NS) approach. Here the also the reservation is performed for high priority service, but the reservation as strict in this sense that services can not access any additional resources besides what was reserved.

Below the results for various levels of reservation in allocation *scheme 1* are presented. The results are obtained by increasing the reservation for *service 1* from zero channels to 16 channels. Fig. 6.2(a) shows the change in delay probability for both services as the number of reserved channels grows, prioritisation of the *service 1* is clearly visible. Similar prioritisation can be noticed in Fig. 6.2(b), Fig. 6.2(c), Fig. 6.2(d), and Fig. 6.2(e) where respectively Mean Waiting Time, Mean Queue Lenth, Blocking probability, and Full-service probability are considered. Especially when *service 1* reservation exceeds 14 channels the penalty for *service 2* is particularly high.

For comparison, Fig. 6.3(a) to Fig. 6.3(e) present the results for *scheme 2* i.e., a similar scenario, with the same total number of channels where the reservations are strict and different flows cannot utilize resources of neighbouring reservations. Since no sharing is possible in this scenario, the reservation of channels for *service 1* only considered range from 6 to 16. Presenting performance analysis for reservations below 6 channels has no sense, as with 10 [erlang-channels] of offered traffic, the results of blocking/delay probabilities, waiting time, and queue length will be extremely high. In fact one can also notice that for *service 1* reservation in the range from 6 to 10 channels, the blocking probability

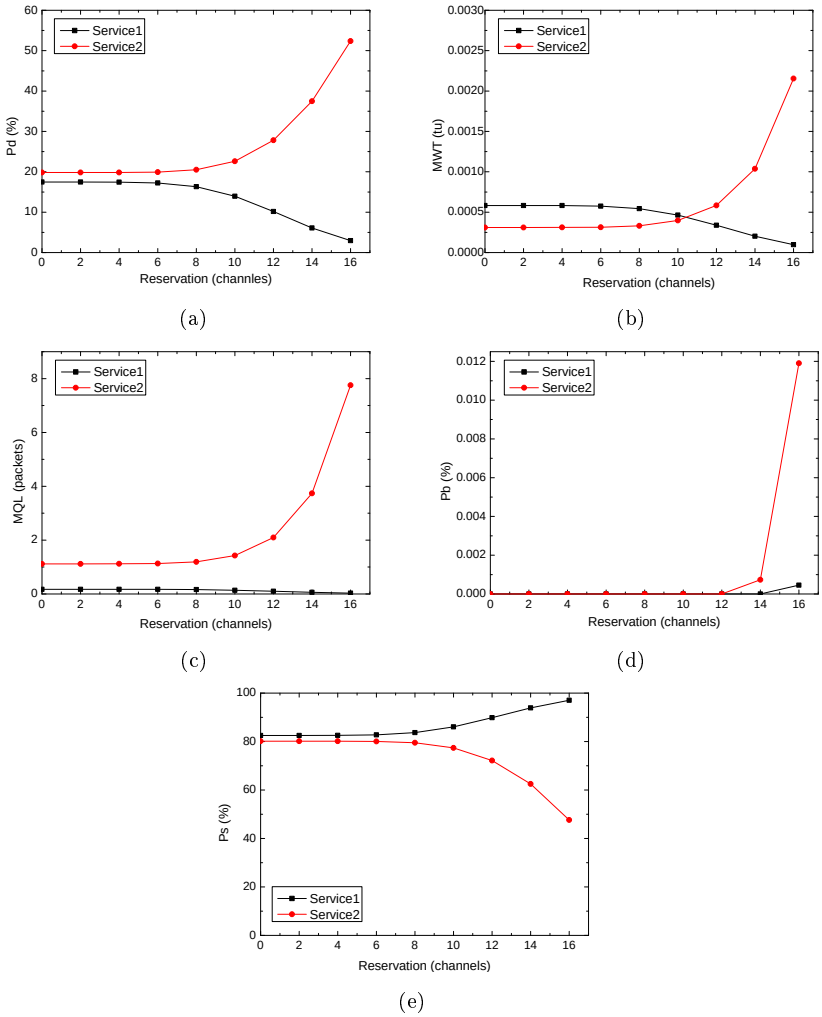


Figure 6.2: Prioritisation of *service 1* and *service 2* as a function of number of reserved channels: (a) Delay probability, (b) Mean waiting time, (c) Mean queue length, (d) Blocking probability, and (e) Full-service probability

(Pb) in Fig. 6.3(d) is high. In Fig. 6.3(a) for this reservation range the probability of delay (Pd) is initially increasing and then dropping again once 12 channels were reserved. Initial growth in delay probability is a consequence of the fact that with lowering blocking probability more

packets spend a lot of time in the queue. Once the blocking is lowered and stable, the delay probability folows expected tendency, i.e., it is decreasing as more channels are reserved for *service 1*.

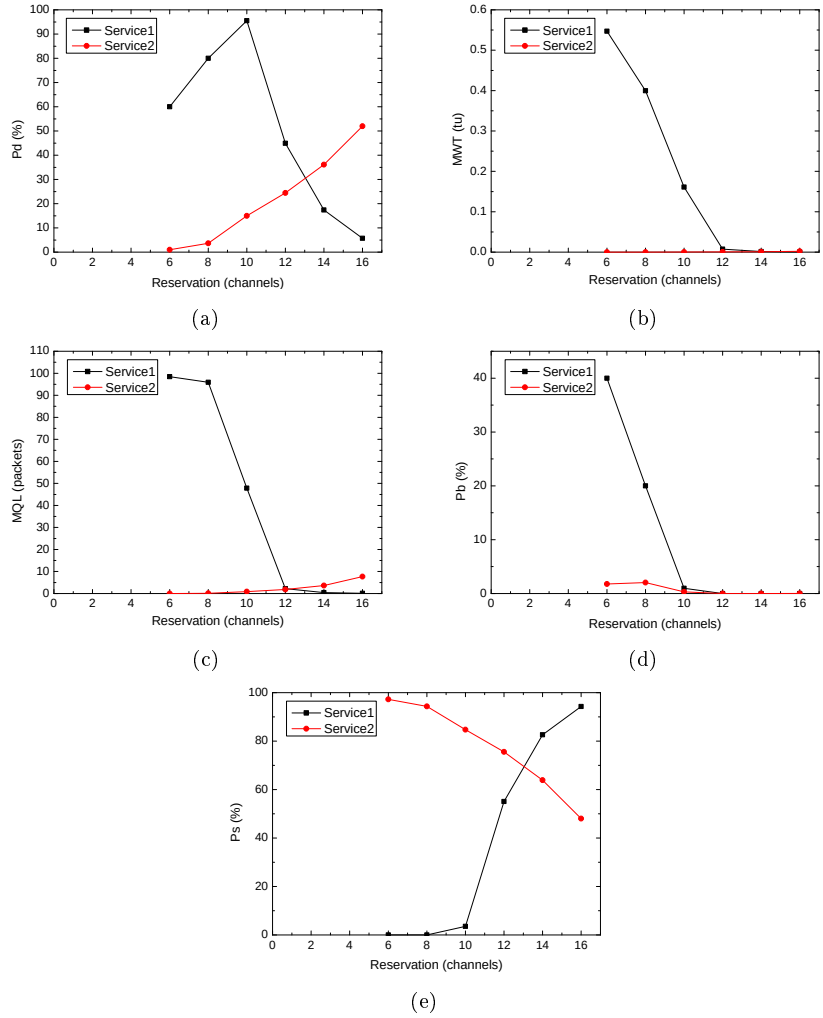


Figure 6.3: Prioritisation of *service 1* and *service 2* as a function of number of reserved channels with *no sharing*: (a) Delay probability, (b) Mean waiting time, (c) Mean queue length, (d) Blocking probability, (e) and Full-service probability

From the above figures it is clear that the reservation with sharing

enabled gives much better results with regards to all parameters considered. When no sharing of the resources is enabled and the reservation for *service 1* is below 10 channels, its delay and blocking probability is naturally very high. At the same time, since almost all the channels for this resource distribution are given to *service 2*, the delay and blocking probabilities, mean waiting time, and queue length of this service are lower.

The important conclusion that can be drawn from Fig. 6.2 and Fig. 6.3 is that enabling resource sharing lowers the blocking and delay penalty in case of bandwidth reservation miscalculation or in case of burst traffic occasionally exceeding the reservation. Simultaneously, in the approach presented here, a minimum of resources can be guaranteed, which depending on the traffic type can keep the service associated with this traffic usable. In this way "partial" reservation can guarantee a certain level of connectivity and at the same time enables resource sharing and statistical multiplexing in the additional pool of resources.

6.4.2 Network of nodes

Open networks

In this section a network of six nodes is considered. There are four sources of traffic, two sources associated with *service 1* and two with *service 2*. One of each is sending traffic to node 1 and 2. The sources generate Poisson traffic and the network is an example of an open queueing network [119]. The topology of the network and routing of the traffic for different services is presented in Fig. 6.4.

For the above described network and services, a comparison of partial reservation with explicit reservation is presented. The partial reservation approach is utilizing reduction factor calculation for distributing the common resources between different services.

Below the results for different channels reservation approaches are presented for all the nodes in the network. If 90% utilisation is considered, Fig. 6.5 presents the results for blocking probability for all the nodes in two scenarios: with no sharing depicted in Fig.6.5(a), and sharing showed in Fig.6.5(b). Considering e.g., node 1 with 45 channels in total and no sharing scenario, 11 channels are dedicated for 10 [erlang-channels] offered by *service 1* while the remaining 34 channels are ded-

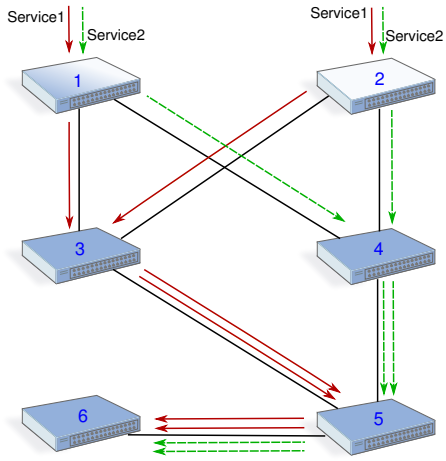
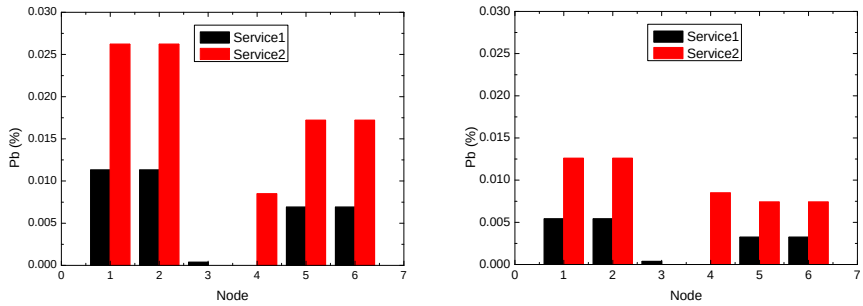


Figure 6.4: Queueing network topology

icated to *service 2*. On the other hand, in case of sharing enabled, the reservation of 10 channels is performed for *service 1*, no channels are dedicated for *service 2*, and there are 35 channels that can be accessed by both services. It is clearly visible that in nodes where both services are accessing resources (i.e., nodes 1, 2, 5 and 6), reservation with sharing lowers the blocking probability significantly.

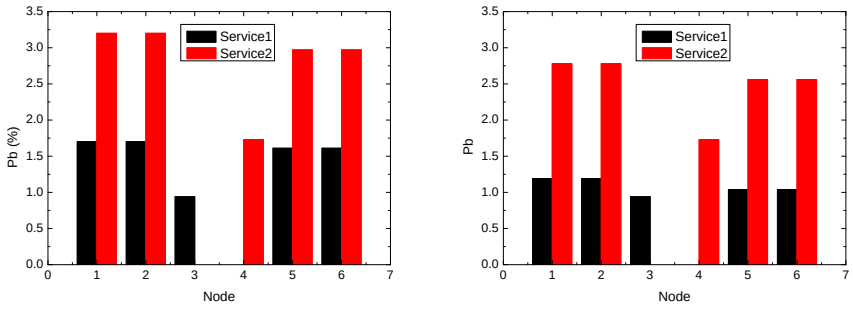


(a) (b)

Figure 6.5: Blocking probability for all the nodes with 90% utilization (a) no sharing and (b) with sharing

If a system for some reasons needs to deal with higher load and

reaches 100% utilization the blocking probability will increase. From Fig. 6.6 it can be noticed that the blocking probability values are significantly higher in comparison with 90% utilisation. Though it is not as significant difference as in Fig. 6.5, one can still notice that the blocking probability in all the nodes is lower for the reservation with sharing.

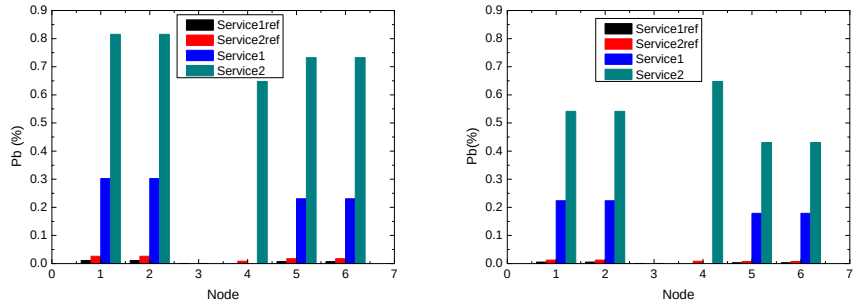


(a) (b)

Figure 6.6: Blocking probability for all the nodes with 100% utilization (a) no sharing and (b) with sharing

The remaining part of this section considers service protection. First, a case where sharing is disabled is evaluated. It is assumed that the reservation for the *service 1* exceeds by 10% its original offered traffic i.e., approx. 90% utilisation is achieved (in other words e.g., in node 1 11 channels are reserved for 10 [erlang-channels] of offered traffic). At the same time the offered traffic of *service 2* is increased first to 110% of the original value. The blocking probability for this case is showed in Fig. 6.7(a). The figure, as a reference, also shows blocking probability for original case without the increase in *service 2* offered traffic (see Service1ref and Service2ref). These results with no sharing are compared with the results when sharing is enabled, and reservation *service 1* is lower. The amount of resources reserved for *service 1* is equal to its offered traffic, while the remaining resources are shared by both services. The results are presented in Fig. 6.7(b). One can notice that even though less resources are dedicated to *service 1*, the blocking probability for this service is lower for the smaller reservation but with part of resources accessible for both services.

Of course, also a drawback of this approach should be considered. Since the reservation for scenario with sharing (WS) is equal to the



(a) (b)

Figure 6.7: Blocking probability for all the nodes with increased *service 2* offered traffic to 110% (a) no sharing and (b) with sharing

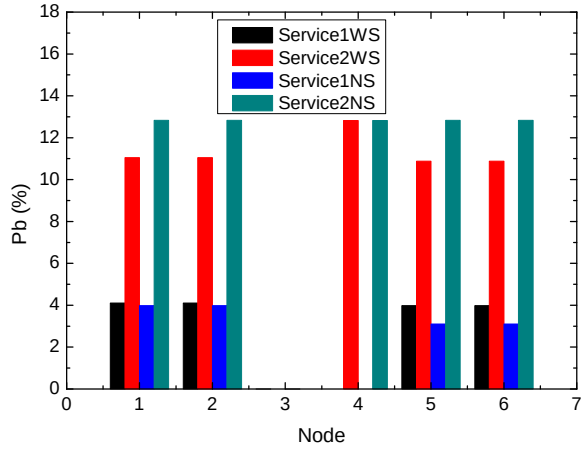


Figure 6.8: Blocking probability for all the nodes with *service 2* offered traffic increased to 130% with sharing (WS) and no sharing (NS)

offered traffic, the blocking probability for this scenario eventually has to be higher comparing to reservation with overhead and no sharing (NS). This situation takes place when the offered traffic in *service 2* reaches 130% of its original value. The blocking probability results for this situation are presented in Fig. 6.8 (see Service1WS and Service1NS).

For cases where the network is dimensioned with larger over-provisioning, the system is a pure delay system (i.e., there is no blocking). It is possible to consider this type of system by e.g., choosing 80% utilisation

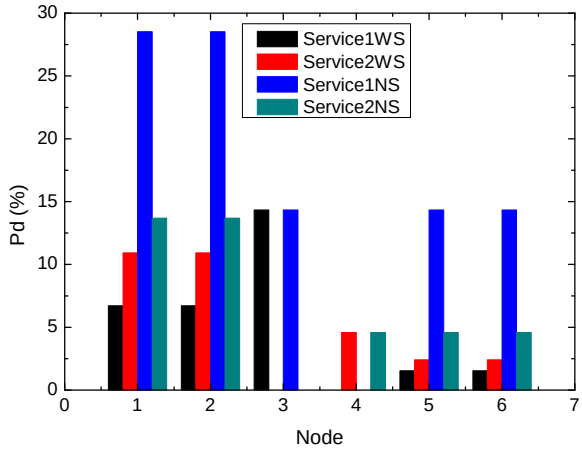


Figure 6.9: Delay probability for pure delay system with sharing (WS) and no sharing (NS)

for *service 1* and limiting the offered traffic in service 2 to 27 [erlang-channels]. In this case the blocking probability is equal to zero, and the delay probability becomes presented in Fig. 6.9. When no sharing is possible, one can observe that the probability of delay of *service 1* traffic is considerably higher in than in the case with smaller reservation and resource sharing.

Closed networks

As described earlier for closed networks the nodes need to be aggregated by multi-dimensional convolution, keeping account of the number of customers in each chain for the aggregated node. The last convolution between the target node and aggregate of all the nodes gives us the performance measurements for the node of interest.

If a closed network like Fig. 6.10 is considered, it is possible to see how different distribution of resources for a partial reservation influence the performance in e.g., node 2. Nodes 1 and 3 have a sufficient amount of channels dedicated for both services (no channels shared) so the packets never experience delay. Mean sojourn services time (MSST) in these nodes are equal to 4 and 8 time-units for *service 1* and *service 2*, respectively. In node 2 there is a reservation performed for the *service 1* traffic.

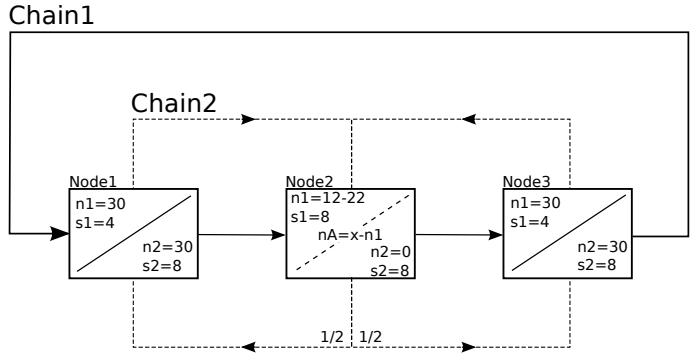


Figure 6.10: Closed network

Table 6.3: Service 1 and 2 waiting time

n1	n2	nA	MSST1	MSST2
12	0	16	8.2364E+00	8.1260E+00
14	0	14	8.2363E+00	8.1261E+00
16	0	12	8.2347E+00	8.1358E+00
18	0	10	8.2159E+00	8.3005E+00
20	0	8	8.1458E+00	9.4119E+00
22	0	6	8.0521E+00	1.3513E+01

There are no resources dedicated for *service 2* traffic, but there are some common resources available for both services. As depicted in Fig. 6.10 the reserved resources for *service 1* change from 12 to 22 channels. The remaining channels a of total 28 are accessible by both services. Table 6.3 presents the results of sojourn service time for *service 1* and *service 2* with different resource distribution. It can be concluded that dedicating more resources for *service 1* traffic limits the additional waiting time. This of course has an impact on the service time for *service 2* which, increases as less channels are accessible.

6.5 Summary

This chapter treated the topic of QoS provisioning on a more generic level, focusing on teletraffic principles. An extension of the model de-

scribed in [121] was presented and used for dimensioning single node, open and closed networks scenarios. Obtaining state probabilities for chains, where minimal resource guarantees are given, allows exact performance measurements and can be used for dimensioning networks with reservations and partial reservations.

Chapter 7

Conclusions and Outlook

The availability of services alone is less and less sufficient to satisfy users' needs and expectations. Service providers acknowledge customers requirements for better quality, in particular when certain delay and packet loss sensitive services are considered. At the same time, since there are limits on bandwidth that can be delivered to a particular site, QoS provisioning is becoming more popular among Internet Service Providers (ISPs). Introducing QoS might be, in some cases a possibility to attract new customers, or on the other hand, a chance to bring more revenue from the existing ones.

However, implementing QoS solutions is not an easy task. To name just some of the difficulties: a number of network domains need to be considered; QoS provisioning is different in home, access and core networks; the closer to the core one gets, the more often scalability is a problem.

This thesis addressed selected of the QoS provisioning issues. First, home QoS provisioning was considered. The focus was mainly given to UPnP-QoS Architecture, but it is important to mention as stated previously, that analyses performed here are generic enough to apply their results to other Service Oriented Architectures (SOAs). When the choice of SOAs is considered, the reason for their use in home environment seems natural. They are very flexible, and quite intuitive in use and configuration, which is a crucial factor from a user-experience point of view. In case a trade-off between overhead and ease of use needs to be made, it might be reasonable to agree on some overhead for the

sake of usability. Even a very efficient system, too complex for intended customers is not much of a use.

Considering UPnP-QoS Architecture, it was demonstrated that it provides good QoS for traffic flows on the signalling layer. It is probably undesired that high priority flows require, on the average, longer time for QoS establishment, however it is balanced with a lower QoS request rejection ratio. One could question the usability of the system where high priority and delay sensitive traffic can experience longer session establishment. But actually, if one examines setup time values obtained taking MoCA-device message parsing time into consideration, the difference in setup time for high and low priorities is not that significant. It can be argued that a 20% delay overhead significantly lowering the rejection probability is fair. When the setup time values alone are discussed, then by comparison of data with and without XML parsing, it seams like the parser is the main contributor to setup delay. Since the setup time presented has some room for improvement (considering the compact size of modelled network), one should put a lot of emphasis on the capabilities of devices included in the network (especially in regards to message processing).

Next, the queueing delay at the packet level was considered. The idea behind this verification was to see what is the influence of implementing UPnP-QoS on devices with different queueing mechanisms. The hypothesis that more advanced queueing techniques give only marginal improvement for networks with traffic admission control was confirmed. Of course, the size of the network is a factor. The data presented in this thesis consider two hops only (reasonable for home network). The benefits from having a more efficient queueing mechanism would be more visible in a bigger network. An overall conclusion could be that for end-devices with limited processing power or energy constraints, there is no need for more advanced queueing techniques in cases when UPnP-QoS performs the access control. At the same time the network components (i.e., not the *end-devices*) should be capable of scheduling traffic in more efficient ways.

Following this UPnP-QoS analysis, some unaddressed issues of this architecture were studied. Three preemption algorithms, suitable for integration with UPnP-QoS signalling, were proposed. The algorithms were compared considering: pre-emption rate, rejection rate, network

utilization, and exceeding bandwidth release. After reviewing the results it was the Minimal Single Fit algorithm that was identified as the most suitable for use within home architecture. Though Minimal Group Fit gives better results when high priority flows are considered, they are achieved for a price of higher computational complexity. The preemption study also proposes an approach where a preemption algorithm is chosen depending on network conditions or QoS request state. Running a different preemption algorithm depending on the situation can lower the average complexity, while providing required QoS to particular flow groups. This was demonstrated by using the request's priority for making a choice between Minimal Single Fit and Minimal Group Fit algorithms.

Next proposed extension to UPnP-QoS was a Network Based Control Point. This component addresses the issue of non-compliant with UPnP-QoS devices in the home network. Among available methods to deal with such devices and preserve QoS, the auto-classification of traffic seems to be an interesting idea with a lot of potential. It is clearly challenging but simulations show that the results for QoS control are satisfactory. With 90-95 percent auto-classification accuracy one can control the network almost as for fully UPnP-QoS compliant environment. In case of lower accuracies the benefits are not straight forward. For short traffic sessions the signalling and detection overhead is also becoming a factor, and the impact of the classifier might be insignificant.

Detailed consideration of home QoS has also an important influence on QoS in other domains. As mentioned before, the closer one gets to core networks, the bigger issue the scalability becomes. Additionally, with growing traffic volume there is a tendency to place decision making functionality at the network edges. This thesis presents the possibility of initiating the QoS provisioning in a home device. The studies of mapping QoS parameters between home and access networks are focused on tightening the cooperation between UPnP-QoS and Generalized Multi-Protocol Label Switching (GMPLS) networks. In order to allow mapping of the QoS parameters between domains, UPnP initiated LSP establishment was proposed and designed. The idea was to use a virtual UPnP-QoS device that would take the UPnP-QoS request and modify its parameters in such a way that by connecting to GMPLS control plane this virtual device could initialise the LSP setup in a GMPLS part of the network. The performed tests verify that designed interface can,

by proper interaction with UPnP-QoS setup, establish LSPs in multi-layer Ethernet test-bed. To fully benefit from interdomain QoS setup, a close interaction between UPnP-QoS and GMPLS is necessary, and bidirectional exchange of QoS information is required. The studies show that with virtually no modifications, UPnP-QoS and GMPLS are a great match enabling interdomain QoS provisioning.

Further exploring GMPLS and its versatility, a study of GMPLS controlled Ten Gigabit Passive Optical Network (XG-PON) was presented. As PON networks are a popular choice among network operators, they should not be left unaddressed. With UPnP-QoS/GMPLS mapping at hand and high popularity of GMPLS in core networks, it was interesting to verify the possibility of controlling XG-PON using GMPLS - enabling an end-to-end control suite. As a matter of fact, GMPLS can be used for controlling XG-PON, and with extended number of XGEM Ports and Alloc-IDs (in comparison to GPON), the flexibility of LSP establishment is high enough to allow per flow resource reservation.

Finally, a more generic approach was used with core networks in mind. Queueing networks, both open and closed, were analysed for multi-rate and multi-service traffic with a reduction factor. Enabling flexible reservations for traffic like video, may improve blocking and delay probability. The study presents the exact solution to the problem of applying the reduction factor for cases where multiple services compete for resources, and some services a have a number of channels reserved exclusively for their use. Results show that "partial reservations" combined with the reduction factor for overlay capacity lowers the blocking and delay probability for both services: the background service and most importantly the prioritised service.

To conclude, there were numerous aspects of QoS covered in this thesis - moving the focus from home networks through the access towards the core, and then shifting to generic resource allocation problems. Not a trivial part of this thesis was focused on mapping QoS parameters between different technologies and domains in attempt to bring the end-to-end QoS provisioning closer to reality. Hopefully in the future, designers and administrators of different domains will provide a generic subset of QoS mechanisms allowing interoperability of different networking technologies, like it was presented in this thesis for the chosen technologies.

Bibliography

[1] A. Odlyzko, "The economics of the Internet: Utility, utilization, pricing, and Quality of Service," Tech. Rep., 1999.

[2] K. Nahrstedt, "To overprovision or to share via QoS-aware resource management?" in *High Performance Distributed Computing, 1999. Proceedings. The Eighth International Symposium on*, 1999, pp. 205 –212.

[3] J. Roberts, "Internet traffic, QoS, and pricing," *Proceedings of the IEEE*, vol. 92, no. 9, pp. 1389 – 1399, sept. 2004.

[4] C. DeCusatis and L. Jacobowitz, "Quality of service for converged data and voice over IP networks," IBM Corporation.

[5] F. Baker and J. Polk, "Implementing an emergency telecommunications service for real-time services in the Internet protocol suite," RFC 4542 (Informational), Internet Engineering Task Force, May 2006, updated by RFC 5865.

[6] "Cisco Visual Networking Index: Forecast and Methodology, 2010-2015 - White Paper," Cisco, 2011.

[7] S. Blake, D. Black, M. Carlson, E. Davies, Z. Wang, and W. Weiss, "An Architecture for Differentiated Service," RFC 2475 (Informational), Internet Engineering Task Force, December 1998, updated by RFC 3260.

[8] R. Braden, D. Clark, and S. Shenker, "Integrated Services in the Internet Architecture: an Overview," RFC 1633 (Informational), Internet Engineering Task Force, Jun. 1994.

[9] M. Rose and D. Cass, "ISO Transport Service on top of the TCP Version: 3," RFC 1006 (Standard), Internet Engineering Task Force, May 1987, updated by RFC 2126.

[10] L. Brewka, H. Wessing, and L. Dittmann, "Signaling performance of UPnP QoS Architecture," in *Advanced Networks and Telecommunication Systems (ANTS), 2009 IEEE 3rd International Symposium on*, dec. 2009, pp. 1 –3.

[11] R. Fu, M. Berger, Y. Zheng, L. Brewka, and H. Wessing, "Next Generation Network based Carrier Ethernet test bed for IPTV traffic," in *EUROCON 2009, EUROCON '09. IEEE*, May 2009, pp. 1781 –1787.

[12] H. Wessing, M. Berger, H. Yu, A. Rasmussen, L. Brewka, and S. Ruepp, *Evaluation of Network Failure induced IPTV degradation in Metro Networks*, ser. Electrical and Computer Engineering Series. World Scientific and Engineering Acad and Soc, 2009, pp. 135–139.

[13] G. Kardaras, J. Soler, L. Brewka, and L. Dittmann, "Fiber to the antenna: A step towards multimode radio architectures for 4G mobile broadband communications," in *Fourth IEEE International Conference on Advanced Networks and Telecommunication Systems (ANTS) (IEEE ANTS 2010)*, Mumbai, India, 12 2010.

[14] L. Brewka, H. Wessing, and L. Dittmann, "Evaluation of lightweight preemption algorithms for UPnP QoS Architecture," in *Communications and Networking in China (CHINACOM), 2010 5th International ICST Conference on*, August 2010, pp. 1 –5.

[15] J. Nelis, D. Verslype, C. Develder, L. Brewka, H. Wessing, and L. Dittmann, "Bandwidth reservations in home networks: Performance assessment of UPnP-QoS V3," in *Local Computer Networks (LCN), 2010 IEEE 35th Conference on*, Oct. 2010, pp. 272 –275.

[16] M. Popov, A. Gavler, P. Sköldström, and L. Brewka, "Integration of qos provisioning in home and access networks," in *Access Networks and In-house Communications*. Optical Society of America, 2010, p. AWB6.

[17] L. Brewka, H. Wessing, and L. Dittmann, "UPnP QoS and queuing in home networks," in *Quality of Service (IWQoS), 2010 18th International Workshop on*, Jun. 2010, pp. 1 –2.

[18] H. Wessing, M. S. Berger, H. M. Gestssson, H. Yu, A. Rasmussen, L. Brewka, and S. Ruepp, "Evaluation of restoration mechanisms for future services using Carrier Ethernet," *WSEAS Transactions on Communications*, vol. 9, pp. 322–331, 2010.

[19] L. Brewka, H. Wessing, A. Rosselló-Busquet, G. Kardaras, and L. Dittmann, "Network Based Control Point for UPnP QoS Architecture," in *The 8th Annual IEEE Consumer Communications and Networking Conference - Multimedia & Entertainment Networking and Services (CCNC'2011 - Multimedia & Entertainment Networking and Services)*, Las Vegas, NV, USA, Jan. 2011, pp. 426–430.

[20] L. Brewka, P. Sköldström, A. Gavler, V. Nordell, H. Wessing, and L. Dittmann, "QoS enabled resource allocation over an UPnP-QoS - GMPLS controlled edge," in *Consumer Communications and Networking Conference (CCNC), 2011 IEEE*, Las Vegas, NV, USA, Jan. 2011, pp. 218 –222.

[21] L. Brewka, H. Wessing, and L. Dittmann, "UPnP QoS Architecture and lightweight preemption algorithms," in *Consumer Communications and Networking Conference (CCNC), 2011 IEEE*, Las Vegas, NV, USA, Jan. 2011, pp. 234 –236.

[22] A. Rosselló-Busquet, L. J. Brewka, J. Soler, and L. Dittmann, "OWL Ontologies and SWRL Rules Applied to Energy Management," in *Computer Modelling and Simulation (UKSim), 2011 UkSim 13th International Conference on*, 30 2011-april 1 2011, pp. 446 –450.

[23] J. Soler, A. Rosselló-Busquet, L. Brewka, M. S. Berger, and L. Dittmann, "Networks and services: A decade's perspective." *Advances in Next Generation Services and Service Architectures*, October 2010.

[24] L. Brewka, P. Sköldström, A. Gavler, V. Nordell, H. Wessing, and L. Dittmann, "ALPHA: Proposal of mapping QoS parameters between UPnP home network and GMPLS access," in *SELFMAGIC-NETS Workshop, part of International ICST Conference on Access Networks (AccessNets) - 5*, Budapest, Hungary, November 2010.

[25] J. Wang, L. J. Brewka, S. R. Ruepp, and L. Dittmann, "Cross Layer QoS Provisioning in Home Networks," in *Proceedings of OP-NETWORK 2011*, Wasington, USA, 2011.

[26] L. Brewka, A. Gavler, H. Wessing, and L. Dittmann, "Proposal of QoS enabled GMPLS controlled XG-PON," in *2nd Internationale Workshop on Fiber Optics in Access Network - QoS and New applications (FOAN 2011)*, Budapest, Hungary, Oct. 2011.

[27] L. Brewka, P. Sköldström, J. Nelis, C. Develder, and H. Wessing, "Automatic Provisioning of End-to-End QoS into the Home," *Consumer Electronics, IEEE Transactions on*, vol. 57, no. 4, pp. 1670 –1678, November 2011.

[28] L. Brewka, A. Gavler, H. Wessing, and L. Dittmann, "Including 10-gigabit-capable passive optical network under end-to-end generalized multi-protocol label switching provisioned quality of service," *Fiber and Integrated Optics*, vol. 31, no. 2, pp. 133–146, 2012.

[29] P. Larouche, "Law and technology: The network neutrality debate hits Europe," *Commun. ACM*, vol. 52, pp. 22–24, May 2009.

[30] S. S. Benjamin Teitelbaum, "Why premium IP service has not deployed (and probably never will)," May 2002.

[31] "Enterprise QoS Solution Reference Network Design Guide," Cisco.

[32] A. Meddeb, "Internet QoS: Pieces of the puzzle," *Communications Magazine, IEEE*, vol. 48, no. 1, pp. 86 –94, January 2010.

[33] N. L. Sauze, A. Chiosi, R. Douville, H. Pouyllau, H. Lonsethagen, C. P. Fantini, Palasciano, A. Cimmino, M. A. C. Rodriguez, O. Dugeon, D. Kofman, X. Gadefait, P. Cuer, N. Ciulli, G. Carrozzo, A. Soppera, B. Briscoe, F. Bornstaedt, M. Andreou, G. Stamoulis, C. Courcoubetis, P. Reichl, I. Gojmerac, J. L. Rougier,

S. Vaton, D. Barth, and A. Orda, "ETICS: QoS-enabled interconnection for future Internet services," 2010.

[34] Y. Huang and R. Guerin, "Does over-provisioning become more or less efficient as networks grow larger?" in *Network Protocols, 2005. ICNP 2005. 13th IEEE International Conference on*, November 2005, pp. 11 pp. –235.

[35] S. Cheshire, B. Aboba, and E. Guttman, "Dynamic Configuration of IPv4 Link-Local Addresses," RFC 3927 (Proposed Standard), Internet Engineering Task Force, May 2005.

[36] "Zeroconf," http://www.zeroconf.org/.

[37] *Bonjour Overview*, Apple Inc., http://developer.apple.com/ documentation /Cocoa/Conceptual/NetServices/NetServices.pdf, May 2006.

[38] *Internet Grouping and Resource Sharing*, IGRS Information Industry Association, http://www.igrs.org/en/index/index.asp.

[39] *Jini Architecture Specification*, http://www.jini.org/wiki/Jini_Architecture_Specification, March 2007.

[40] *Devices Profile for Web Services Version 1.1*, OASIS, http://docs.oasis-open.org/ws-dd/dpws/wsdd-dpws-1.1-spec.html, July 2009.

[41] "Devices Profile for Web Services," available at: http://specs.xmlsoap.org/ws/2006/02/devprof/devicesprofile.pdf, February 2006.

[42] "Introducing Devices Profile for Web Services," Microsoft Corporation, http://download.microsoft.com/download/b/5/3/b53ea430-dbe5-440c-a308-df97b10280b7/introducing_dpws.pdf, 2007.

[43] "UPnP Technology, The Simple, Seamless Home Network, A White Paper," UPnP Forum, http://www.upnp-ic.org/resources/UIC_Marketing-UPnP_Business_Whitepaper.pdf, December 2006.

[44] R. Droms, "Dynamic Host Configuration Protocol," RFC 2131 (Draft Standard), Internet Engineering Task Force, Mar. 1997, updated by RFCs 3396, 4361, 5494, http://www.ietf.org/rfc/rfc2131.txt.

[45] D. Plummer, "Ethernet Address Resolution Protocol: Or Converting Network Protocol Addresses to 48.bit Ethernet Address for Transmission on Ethernet Hardware," RFC 826 (Standard), Internet Engineering Task Force, 1982, updated by RFCs 5227, 5494, http://www.ietf.org/rfc/rfc826.txt.

[46] P. Mockapetris, "Domain names - concepts and facilities," RFC 1034 (Standard), Internet Engineering Task Force, Nov. 1987, updated by RFCs 1101, 1183, 1348, 1876, 1982, 2065, 2181, 2308, 2535, 4033, 4034, 4035, 4343, 4035, 4592, 5936, http://www.ietf.org/rfc/rfc1034.txt.

[47] ——, "Domain names - implementation and specification," RFC 1035 (Standard), Internet Engineering Task Force, Nov. 1987, updated by RFCs 1101, 1183, 1348, 1876, 1982, 1995, 1996, 2065, 2136, 2181, 2137, 2308, 2535, 2845, 3425, 3658, 4033, 4034, 4035, 4343, 5936, 5966, http://www.ietf.org/rfc/rfc1035.txt.

[48] *UPnP Device Architecture 1.0*, UPnP Forum, April 2008.

[49] T. Cai, P. Leach, Y. Gu, and S. Albright, "Simple Service Discovery Protocol," Internet Engineering Task Force, Oct. 1999.

[50] G. Barish and K. Obraczke, "World Wide Web caching: trends and techniques," *Communications Magazine, IEEE*, vol. 38, no. 5, pp. 178 –184, May 2000.

[51] L. Breslau, P. Cao, L. Fan, G. Phillips, and S. Shenker, "Web caching and Zipf-like distributions: evidence and implications," in *INFOCOM '99. Eighteenth Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE*, vol. 1, Mar. 1999, pp. 126 –134 vol.1.

[52] L. Subramanian, I. Stoica, H. Balakrishnan, and R. H. Katz, "OverQoS: offering Internet QoS using overlays," *SIGCOMM*

Comput. Commun. Rev., vol. 33, pp. 11–16, January 2003, http://doi.acm.org/10.1145/774763.774764.

[53] A. Mohammed, E. Jones, H. Ogier, M. Vouk, and Z. Dwekat, "DiffServ experiments: analysis of the premium service over the Alcatel-NCSU Internet2 testbed," in *Universal Multiservice Networks, 2002. ECUMN 2002. 2nd European Conference on*, 2002, pp. 124 – 130.

[54] E. Schonfeld, "Cisco: By 2013 video will be 90 percent of all consumer IP traffic and 64 percent of mobile," CrunchBase Information, June 2009.

[55] *UPnP QoS Architecture:3 Service Template Version 1.01 For UPnP Version 1.0*, UPnP Forum, November 2008.

[56] J. P. Laulajainen, P. Perala, and A. Laikari, "Evaluation Of UPnP QoS Framework Performance in Wireless LAN," in *Consumer Electronics, 2008. ISCE 2008*, April 2008.

[57] MoCA, "Moca," http://www.mocalliance.org/index.php, 2010.

[58] F. Giovanelli, G. Bigini, M. Solighetto, and P. Maggi, "A UPnP-based bandwidth reservation scheme for in-home digital networks," in *ICT 2003. 10th International Conference on Telecommunications*, vol. 2, February 2003.

[59] "UPnP AV Architecture:1, For UPnPTM Version 1.0," UPnP Forum, September 2008.

[60] *UPnP QosManager:3 Service Template Version 1.01 For UPnP Version 1.0*, UPnP Forum, November 2008.

[61] *UPnP QosPolicyHolder:3 Service Template Version 1.01 For UPnP Version 1.0*, UPnP Forum, November 2008.

[62] *UPnP QosDevice:3 Service Template Version 1.01*, UPnP Forum, November 2008.

[63] P. J. Burke, "Priority traffic with at most one queuing class," *Operations Research*, vol. 10, no. 4, pp. 567–569, Jul. 1962.

[64] W. S. Helly, "Two doctrines for the handling of two priority traffic by a group of n," *Operations Research*, vol. 10, no. 2, pp. 268 – 269, Jul. 1962.

[65] L. E. Dor, "On loss systems with preemptive priority," Telrad Telecommunications industrials, 1991.

[66] *OPNET Modeler Version 14.5.A*, http://www.opnet.com.

[67] S. Jeon, R. T. Abler, and A. E. Goulart, "The Optimal Connection Preemprion Algotirhm in a Multi-Class Network," in *IEEE International Conference on Communications, 2002. ICC 2002.*, vol. 4, 2002, pp. 2294–2298.

[68] J. Garay and I. Gopal, "Call preemption in communication networks," in *INFOCOM '92. Eleventh Annual Joint Conference of the IEEE Computer and Communications Societies, IEEE*, vol. 3, New Delhi, India, October 1992, pp. 1043–1050.

[69] T. Shan and O. W. Yang, "Bandwidth management for supporting Differentiated-Service-aware traffic engineering," in *IEEE International Conference on Communications, 2002. ICC 2002.*, vol. 2, September 2002, pp. 1305 – 1309.

[70] V. Stanisic and M. Devetsikiotis, "A Dynamic Study of Providing Quality of Service Using Preemption Policies with Random Selection," in *IEEE International Conference on Communications, 2003. ICC 2003.*, vol. 3, 5 2003, pp. 1543–1546.

[71] T. S. S. O. ITU, "P.800 - methods for subjective determination of transmission quality," INTERNATIONAL TELECOMMUNICATION UNION, August 1996.

[72] M. Roughan, S. Sen, O. Spatscheck, and N. Duffield, "Class-of-service mapping for QoS: a statistical signature-based approach to IP traffic classification," in *IMC '04: Proceedings of the 4th ACM SIGCOMM conference on Internet measurement.* New York, NY, USA: ACM, 2004, pp. 135–148.

[73] M. Dusi, F. Gringoli, and L. Salgarelli, "IP traffic classification for QoS guarantees: The independence of packets," in *Computer*

Communications and Networks, 2008. ICCCN '08. Proceedings of 17th International Conference on, 3-7 2008, pp. 1 –8.

[74] J. Park, H.-R. Tyan, and C.-C. Kuo, "GA-based Internet traffic classification technique for QoS provisionin," in *Intelligent Information Hiding and Multimedia Signal Processing, 2006. IIH-MSP '06. International Conference on*, December 2006, pp. 251 –254.

[75] A. W. Moore and K. Papagiannaki, "Toward the accurate identification of network applications," in *PAM*, 2005, pp. 41–54.

[76] A. W. Moore and D. Zuev, "Internet traffic classification using bayesian analysis techniques," in *SIGMETRICS '05: Proceedings of the 2005 ACM SIGMETRICS international conference on Measurement and modeling of computer systems*, vol. 33, no. 1. New York, NY, USA: ACM, June 2005, pp. 50–60.

[77] D. Antoniades, M. Polychronakis, S. Antonatos, E. Markatos, and S. Ubik, "Appmon: An application for accurate per application network traffic characterization," in *BroadBand Europe*, 2006.

[78] J.-P. Laulajainen and M. Hirvonen, "Automatic QoS control in UPnP home networks," in *ISCC*, 2009, pp. 455–460.

[79] V. Paxson and S. Floyd, "Wide area traffic: the failure of Poisson modeling," *Networking, IEEE/ACM Transactions on*, vol. 3, no. 3, pp. 226 –244, Jun. 1995.

[80] W.-S. Hwang and P.-C. Tseng, "A QoS-aware residential gateway with bandwidth management," *Consumer Electronics, IEEE Transactions on*, vol. 51, no. 3, pp. 840 – 848, Aug. 2005.

[81] J. But, G. Armitage, and L. Stewart, "Outsourcing automated QoS control of home routers for a better online game experience," *Communications Magazine, IEEE*, vol. 46, no. 12, pp. 64 –70, December 2008.

[82] M. Siddiqui, S. Amin, and C. S. Hong, "A set-top box for end-to-end QoS management and home network gateway in IMS," *Consumer Electronics, IEEE Transactions on*, vol. 55, no. 2, pp. 527 –534, May 2009.

[83] R. Good and N. Ventura, "End to end session based bearer control for IP multimedia subsystems," in *Integrated Network Management, 2009. IM '09. IFIP/IEEE International Symposium on*, June 2009, pp. 497 –504.

[84] S. Arrizabalaga, P. Cabezas, J. Legarda, and A. Salterain, "A novel QoS architecture for multi-service provisioning in multi-residential gateways," *Consumer Electronics, IEEE Transactions on*, vol. 55, no. 2, pp. 477 –485, May 2009.

[85] M. Welzl and M. Muhlhauser, "Scalability and quality of service: a trade-off?" *Communications Magazine, IEEE*, vol. 41, no. 6, pp. 32 – 36, June 2003.

[86] *UPnP QosDevice:3 Underlying Technology, Interface Addendum, Service Template Version 1.01, For UPnP Version 1.0*, UPnP Forum, November 2008.

[87] E. Rosen, A. Viswanathan, and R. Callon, "Multiprotocol Label Switching Architecture," RFC 3031 (Proposed Standard), Internet Engineering Task Force, Jan. 2001, updated by RFC 6178, http://www.ietf.org/rfc/rfc3031.txt.

[88] "ITU-T Recommendation G.872: Architecture of optical transport networks," Nov. 2001, http://www.itu.int/rec/T-REC-G.872/en.

[89] "ITU-T, Network node interface for synchronous digital hierarchy (SDH), G.707/Y.1322," Oct. 2000.

[90] D. Awduche, L. Berger, D. Gan, T. Li, V. Srinivasan, and G. Swallow, "RSVP-TE: Extensions to RSVP for LSP Tunnels," RFC 3209 (Proposed Standard), Internet Engineering Task Force, Dec. 2001, updated by RFCs 3936, 4420, 4874, 5151, 5420, 5711, http://www.ietf.org/rfc/rfc3209.txt.

[91] D. Katz, K. Kompella, and D. Yeung, "Traffic Engineering (TE) Extensions to OSPF Version 2," RFC 3630 (Proposed Standard), Internet Engineering Task Force, Sep. 2003, updated by RFCs 4203, 5786, http://www.ietf.org/rfc/rfc3630.txt.

[92] K. Kompella and Y. Rekhter, "OSPF Extensions in Support of Generalized Multi-Protocol Label Switching (GMPLS)," RFC 4203 (Proposed Standard), Internet Engineering Task Force, Oct. 2005, updated by RFCs 6001, 6002.

[93] R. Aggarwal and K. Kompella, "Advertising a Router's Local Addresses in OSPF Traffic Engineering (TE) Extensions," RFC 5786 (Proposed Standard), Internet Engineering Task Force, Mar. 2010.

[94] "Common control and measurement plane," The CCAMP Work group, http://tools.ietf.org/wg/ccamp/.

[95] F. L. Faucheur, L. Wu, B. Davie, S. Davari, P. Vaananen, R. Krishnan, P. Cheval, and J. Heinanen, "Multi-Protocol Label Switching (MPLS) Support of Differentiated Services," RFC 3270 (Proposed Standard), Internet Engineering Task Force, May 2002, updated by RFC 5462, http://www.ietf.org/rfc/rfc3270.txt.

[96] J. Wroclawski, "Specification of the Controlled-Load Network Element Service," RFC 2211 (Proposed Standard), Internet Engineering Task Force, Sep. 1997.

[97] S. Shenker, C. Partridge, and R. Guerin, "RFC 2212: Specification of guaranteed quality of service," Sep 1997.

[98] R. Braden, L. Zhang, S. Berson, S. Herzog, and S. Jamin, "Resource ReSerVation Protocol (RSVP) – Version 1 Functional Specification," RFC 2205 (Proposed Standard), Internet Engineering Task Force, Sep. 1997, updated by RFCs 2750, 3936, 4495.

[99] J. Wroclawski, "RFC 2210: The use of RSVP with IETF integrated services," Sep. 1997, status: PROPOSED STANDARD.

[100] *TR-069 CPE WAN Management Protocol v1.1*, The Broadband Forum, December 2007.

[101] P. Sköldström, A. Gavler, C. P. Larsen, A. Welin, and A. Kern, "The Acreo GMPLS Testbed - Current Functionality and a Path Towards a Multi-Flavoured Ethernet Hierarchy," in *ICT Mobile Summit 2009*, June 2009.

[102] T. Roosendaal, "Big buck bunny," in *ACM SIGGRAPH ASIA 2008 computer animation festival*, ser. SIGGRAPH Asia '08. New York, NY, USA: ACM, 2008, pp. 62–62.

[103] C. Perkins and P. Calhoun, "Authentication, Authorization, and Accounting (AAA) Registration Keys for Mobile IPv4," RFC 3957 (Proposed Standard), Internet Engineering Task Force, Mar. 2005.

[104] H.-B. Guo and G.-S. Kuo, "A GMPLS- and EPON-based optical access network with end-to-end QoS guarantee for broadband IP services," *Network Architectures, Management, and Applications II*, vol. 5626, no. 1, pp. 207–214, 2005, http://link.aip.org/link/?PSI/5626/207/1.

[105] G. Yong and G. Fan, "GMPLS-based passive optical network," *Network Architectures, Management, and Applications II*, vol. 5626, no. 1, pp. 905–909, 2005, http://link.aip.org/link/?PSI/5626/905/1.

[106] H.-B. Guo and G.-S. Kuo, "Support of IP micro-mobility in GMPLS and EPON-based integrated network access architecture," in *Communications, 2005. ICC 2005. 2005 IEEE International Conference on*, vol. 3, May 2005, pp. 1863 – 1868 Vol. 3.

[107] ITU-T, "10-Gigabit-capable passive optical network (XG-PON) systems: Definitions, abbreviations and acronyms," 2010.

[108] ——, "Gigabit-capable passive optical networks (GPON): General characteristics," 2008.

[109] ——, "10-Gigabit-capable passive optical networks (XG-PON): Transmission convergence (TC) specifications: 987.3," 2010.

[110] K. Shiomoto, R. Papneja, and R. Rabbat, "Use of Addresses in Generalized Multiprotocol Label Switching (GMPLS) Networks," RFC 4990 (Informational), Internet Engineering Task Force, Sep. 2007, http://www.ietf.org/rfc/rfc4990.txt.

[111] A. Dhaini, C. Assi, A. Shami, and N. Ghani, "Adaptive fairness through intra-ONU scheduling for Ethernet Passive Optical Net-

works," in *Communications, 2006. ICC '06. IEEE International Conference on*, vol. 6, june 2006, pp. 2687 –2692.

[112] K. Iniewski, *Convergence of Mobile and Stationary Next-Generation Networks.* John Wiley & Sons Inc., 2010.

[113] IDATE, "FTTx Market Report," IDATE Consulting & Research, July 2009.

[114] M. Decina and T. Toniatti, "On bandwidth allocation to bursty virtual connections in ATM networks," in *Communications, 1990. ICC '90, Including Supercomm Technical Sessions. SUPERCOMM/ICC '90. Conference Record., IEEE International Conference on*, Apr. 1990, pp. 844 –851 vol.3.

[115] R. Zhang, R. Ruby, J. Pan, L. Cai, and X. Shen, "A hybrid reservation/contention-based MAC for video streaming over wireless networks," *Selected Areas in Communications, IEEE Journal on*, vol. 28, no. 3, pp. 389 –398, Apr. 2010.

[116] G. L. Choudhury, "Analysis of combined voice/data/video operation in cable and DSL access networks: graceful degradation under overload," *Performance Evaluation*, vol. 52, no. 2-3, pp. 89 – 103, 2003, internet Performance and Control of Network Systems.

[117] I. D. Moscholios and M. D. Logothetis, "The Erlang multirate loss model with Batched Poisson arrival processes under the bandwidth reservation policy," *Computer Communications*, vol. 33, no. Supplement 1, pp. S167 – S179, 2010, special Issue: Heterogeneous Networks: Traffic Engineering and Performance Evaluation.

[118] M. Stasiak and M. Głąbowski, "A simple approximation of the link model with reservation by a one-dimensional Markov chain," *Performance Evaluation*, vol. 41, no. 2-3, pp. 195 – 208, 2000.

[119] V. B. Iversen, *Teletraffic Engineering and Network Planning.* Department of Photonic Engineering, Technical University of Denmark, 2010, http://oldwww.com.dtu.dk /education /34340 /material/ telenook.pdf.

[120] ——, "Reversible fair scheduling: the teletraffic theory revisited," in *Proceedings of the 20th International Teletraffic Congress ITC 20*, 2007.

[121] V. B. Iversen and K. King-Tim, "Algorithm for queueing networks with multi-rate traffic," in *Conference Proceedings of First European Teletraffic Seminar (ISBN: 978-83-925375-5-7)*, Poznan, Poland, 2011.

[122] E. Iliakis and G. Kardaras, "Resource allocation in next generation internet," Master's thesis, Technical University of Denmark, 2007.

List of Acronyms

AAA	Authentication, Authorization and Accounting
ACP	Automatic Control Point
Alloc-ID	Allocation Identifier
AON	Active Optical Network
AS	Autonomous Systems
ARP	Address Resolution Protocol
ARQ	Automatic Repeat reQuest
BWmap	bandwidth map
CBQ	Class Based Queuing
CIR	Committed Information Rate
CM	Control and Managemet
CoS	Class of Service
CP	Control Point
DBA	Dynamic Bandwidth Allocation
DHCP	Dynamic Host Configuration Protocol
DiffServ	Differentiated Services
DLNA	Digital Living Network Alliance

DNS	Domain Name Server
DPWS	Device Protocol for Web Services
DSCP	Differentiated Services Code Point
EPON	Ethernet PON
ERO	Explicit Route Object
FEC	Forward Error Correction
FIFO	First In, First Out
FTTH	Fibre to the Home
GMPLS	Generalized Multi-Protocol Label Switching
GPON	Gigabit PON
HG	Home Gateway
HTB	Hierarchical Token Bucket
IETF	Internet Engineering Task Force
IGRS	Intelligent Grouping and Resource Sharing
IntServ	Integrated Services
ISP	Internet Service Provider
LER	Label Edge Router
LSP	Label Switched Path
LSR	Label Switched Router
mDNS	Multicast Domain Name Server
MPLS	Multi-Protocol Label Switching
MoCA	Multimedia over Coax Alliance
MOS	Mean Opinion Score

NBCP	Network Based Control Point
NBMA	Nonbroadcast Multiaccess
OA	Ordered Aggregate
OAM	Operations Administration and Maintenance
OLT	Optical Line Terminal
OMCC	Optical Network Unit Management and Control Channel
ONU	Optical Network Unit
OTN	Optical Transport Network
PON	Passive Optical Network
QD	QoS Device
QM	QoS Manager
PHB	Per Hop Behavior
PIR	Peak Information Rate
PSC	Per Hop Behavior Scheduling Class
QoS	Quality of Service
QPH	QoS Policy Holder
QRG	QoS-aware Residential Gateway
RFC	Request for Comments
RSpec	Receivers Specification
RSVP	Resource ReserVation Protocol
RSVP-TE	Resource ReserVation Protocol with Traffic Engineering
SDH	Synchronous Digital Hierarchy

SOA	Service Oriented Architecture
SR-DBA	Status Reporting DBA
SSDP	Simple Service Discovery Protocol
T-CONT	Transmission Container
TC	Traffic Control
TIN	Traffic Importance Number
TM-DBA	Traffic Monitoring DBA
TSpec	Traffic Specification
UDP	User Datagram Protocol
UIN	User Importance Number
UPnP	Universal Plug and Play
UPnP-QoS	Universal Plug and Play - Quality of Service
URL	Uniform Resource Locator
VoD	Video on Demand
XML	Extensible Markup Language
XGEM	XG-PON Encapsulation Method
XGTC	XG-PON Transmission Convergence
XG-PON	Ten Gigabit Passive Optical Network